THE INTERNET'S IMPACTS ON POWER DIFFERENTIALS IN SECURITY AND CONFLICT

by
Megan L. Ortagus

A thesis submitted to Johns Hopkins University in conformity with the requirements for the degree of Master of Arts in Global Security Studies

Baltimore, Maryland
May 2014

ABSTRACT

Through case studies and empirical statistical research, this thesis tests the theory that information and communications technologies (ICT), specifically the Internet, is a casual factor in shifting the global balance of power away from dominant states towards individuals and smaller states. The Internet affords acute advantages to individuals and smaller states, but it has yet to prove decisive against an armed nation state with the will to use violence, particularly in the case of aggressive authoritarian states. This thesis argues that while ICT exposes states to new security threats and a transference in power may be underway, the current evidence suggests that a dominant nation state's security apparatus is still a more potent force, for now.

These conclusions were reached through a holistic examination of ICT's impact on security through the lenses of state versus state conflict (interstate), citizen-led revolutionary movements (intrastate), and violent non-state actors against the system ("extrastate"). However, this thesis found no conclusive data to support the notion that the Internet is concurrently revolutionizing interstate, intrastate or extrastate conflict to the point whereby a weaker adversary can achieve a desired political outcome through the unique use of cyber tools. While cyberspace adds a new virtual dimension to conflict, much like airpower added a third dimension to military conflict after World War I, cyber weapons have not yet developed to the point where they can replace weaponry in the physical domains. The Internet has neither fundamentally altered human nature nor the desires and

competitions that fuel conflict; it may be transforming the *experience* of conflict, but not necessarily the *outcomes*.

Thesis Readers: Dr. Ariel Roth and Dr. Lee Drutman

ACKNOWLEDGMENTS

The completion of this thesis would be impossible without the unconditional love and support that I received from my husband, Farook. Thank you for your unselfish devotion and patience during this lengthy process.

I would also like to express my appreciation for the faculty at the Johns Hopkins University for providing superb lectures and instruction that always challenged me to think critically; with special thanks to Professors Leila Austin, Charles Blair, Daniel Kuehl, and Ariel Roth.

Table of Contents

INTRODUCTION

A new phenomenon is altering the human experience: the rapid development and deployment of information and communication technologies (ICT) has changed human behavior by transforming information distribution, commerce, and culture.[1] These technologies have affected life for billions of Internet users, and even have indirect impacts on those people without direct access to the Internet.[2] Furthermore, unlike any other form of mass media in history, the Internet is an open platform where users both consume and produce information.[3] While it is clear that the Internet has meaningfully affected particular aspects of modern society, exactly how these technologies are reshaping warfare, terrorism, and civil uprisings remains unsettled. The Internet has brought core structural changes to societies, with profound implications for the security of nation states.

Through case studies and empirical statistical research, this thesis tests the theory that ICT, specifically the Internet, is a casual factor in shifting the global balance of power away from dominant states towards individuals and smaller states. If so, shifting power dynamics will be manifested in interstate conflict, dissident movements, and non-state actor ambitions: wars will be fought differently, citizens will have more leverage over authoritarian states, and transnational groups will approach parity with states in the international system. An important

[1] Benkler, Yochai. *The Wealth of Networks* (New Haven: Yale University Press, 2006), 1.
[2] Nye, Joseph. "Cyber Power", http://web.mit.edu/ecir/pdf/nye-cyberpower.pdf (accessed October 16 2010).
[3] "A Virtual Counter-Revolution," *The Economist*, September 4, 2010, 76.

determining factor for judging ICT's effects on traditional security constructs is the manner by which states and individuals adapt to new power differentials.

The information age presents unique vulnerabilities for dominant players, which lesser ones have had some success in exploiting. However, this thesis will argue that while ICT exposes states to new security threats and a transference in power may be underway, the current evidence suggests that a dominant nation state's security apparatus is still a more potent force, for now. The Internet affords acute advantages to individuals and smaller states, but it has yet to prove decisive against an armed nation state with the will to use violence, particularly in the case of aggressive authoritarian states. As this thesis will demonstrate, this overarching conclusion was reached through a holistic examination of ICT's impact on security through the lenses of state versus state conflict (interstate), citizen-led revolutionary movements (intrastate), and violent non-state actors against the system ("extrastate")[4], each of which will be examined in a distinct chapter.

Chapter one addresses a high-profile policy topic in Washington today: the degree to which cyberwar is now central to interstate conflict. This chapter compares and contrasts the debates between theorists on the substantive consequences of the Internet on war, including the ramifications for how militaries will now define war, the very nature of war, and how power is distributed among armed states. Does the Internet have inherent transformative properties that will render other forms of warfare irrelevant and level the playing field for weak states

[4] "Extrastate" is term created for this paper to juxtapose the variant transnational non-state actor conflict against the better defined interstate and intrastate conflicts.

due to ICT's low cost of entry? Or is the Internet simply an inchoate tool in any state's arsenal, and not coercive enough to result in new military elites?

The first chapter attempts to contextualize cyber warfare by discussing the geopolitical contests from which it arose. It uses a theoretical framework first posited by Eliot Cohen 1996 to evaluate two key interstate conflicts with prominent cyber elements between Russia and Estonia in 2007, then Russia and Georgia in 2008. The chapter concludes that cyber warfare, as deployed by Russia, did not meet all of Cohen's tests for a transformational military technology. The Russian cyber attacks against Estonia inflicted temporary pain, but were insufficiently coercive to produce the desired political outcome. The cyber attacks against Georgia served as a force multiplier for Russia's overwhelmingly superior conventional military, but there is no evidence to indicate the outcome would have differed without the cyber campaign. Russia's limited cyber victory in Estonia was bloodless, but also far less efficacious than its conventional military success. In these case studies, the singular use of the Internet to conduct cyber attacks did not alter countries' power position, nor did it dramatically revolutionize how wars are fought between nation states.

The case studies from chapter one were chosen from the available literature since they represent interstate conflicts with well-documented cyber attacks by which a nation state attempted to achieve a political goal, setting them apart from routine cyber criminality and cyber espionage or sabotage. Further, Russia's conflict with Georgia provides an opportune control case to contrast with its conflict with Estonia in analyzing the impact of ICT on intrastate conflict.

The conclusions reached as a result of examining these two case studies are by no means definitive and further research is necessary, especially as cyber weapons evolve and nation states build more formidable cyber defenses. Of note, chapter one was completed in the fall of 2013, before the conflict between Russia and Ukraine over Crimea in spring 2014. Future research should evaluate the cyber elements in this crisis against Cohen's framework.

Chapter two explores the Internet phenomenon and its effects on internal state security to determine if ICT is altering existing power dynamics between the individual and the state. This chapter is primarily concerned with the argument that the Internet creates a competitive advantage for dissidents inside authoritarian states, which would in turn make revolutions more likely.[5] It categorizes the incipient schools of thought on the Internet to build an intellectual framework in which critical questions can be addressed: Is there a new causal relationship between ICT and successful revolutionary movements? If individuals have more access to ICT in authoritarian states, is the likelihood of revolution increased?

The second chapter analyzes instances of collective ICT usage by Green Movement protestors in Iran following the 2009 Presidential elections to determine whether the Internet was working to the advantage of the agency or the state. For a more nuanced understanding, this chapter also examines the historical relevance of earlier communications tools, such as the telegraph, cassette tape, and television, in Iran during prior reform and revolutionary movements, notably the 1890s tobacco

[5] The term "competitive advantage" is one I have borrowed from economics, specifically Michael Porter's 1990s theory, and applied to the ICT phenomenon. For the purposes paper, competitive advantage implies that citizens could possess technologies that allow them to have an edge over the traditional nation state.

protests and the 1979 revolution. Both of these are control cases that enabled the evaluation of ICT's impact on revolution, as compared to prior developments in communications technology.

The findings from the Iranian case study suggest that from the telegraph to twitter, there is ample historical evidence that communications tools have uniquely enabled the spread of information beyond Iranian state control and have provided dissidents with an open yet underground space to disseminate ideas and to mobilize. Contrarily, as a catalyst for revolutionary movements, the ICT's performance record is unreliable and has only a marginal success rate against nation states like Iran with sophisticated censorship regimes that blunt the Internet's effectiveness for subversion.

In aiming to evaluate the effect of ICT on individual and state power differentials, this thesis chapter required cases that were consistent in popular revolts against governments, providing some correction for differences in cultural variations. Iran offers a very good case with a 5000-year-old civilization and multiple revolutionary attempts within the past 200 years. From within this paradigm, the Green Movement was selected from the abundant literature because it was also the most relevant example of a dissident movement consciously choosing to mobilize based on an Internet utopian philosophy. This philosophy espouses the Internet is a democratizing force that makes traditional organizational structures obsolete, favoring networks over hierarchies. It is a strategy that has failed thus far to bring about revolution in Iran.

Chapter three confronts the post September 11, 2001 conceit that the Internet's pervasive spread of information and ideology has empowered transnational groups against the global political order. Specifically, this chapter evaluates whether ICT has increased the probability that international terrorist organizations will acquire and deploy a weapon of mass destruction (WMD). In chapter three, theory and probability encounter reality in that a terrorist group's increased access to knowledge on the Internet did not enable it to overcome the extent challenges of acquisition and deployment.

Attention to the relationship between violent non-state actors' (VNSA) ICT usage and unconventional weapons is especially important when discussing transnational groups that operate in opposition to the formal nation state system, and seek to overturn the existing order (defined in this paper as "extrastate"). If new media use strongly correlates to increases in VNSA acquisition and deployment of WMD, then it speaks to the Internet's potential influence on 21st century power realignment. A transitional group that obtains even a crude nuclear device is on a more level playing field with nation states, providing it a source of significance and recognition that other forms of terrorism do not afford, thus challenging the alignment of small powers and great powers that has dominated history.

The third chapter tests the aforementioned theory by presenting an empirical analysis of Chemical, Biological, Radiological and Nuclear (CBRN) datasets. It combines a review of three prominent statistical studies with original quantitative analysis to determine if there is in fact a strong correlation between ICT growth and WMD threats. The model created for this paper plots CBRN incidents

from 1990 to 2013 against data on global Internet penetration rates. In this case, the data from the pre-Internet age serves as a control to contrast with more recent terrorist attempts to obtain and use CBRN weapons. The model reveals that the total CBRN linear trend line is slightly decreasing over the time plotted, but is probably more prudently classified as flat due to the small-*n* sample size of the available data. Thus, there is no evident correlation between the rising number Internet users and terrorist attempts to acquire CBRN despite conventional wisdom's suggestion that knowledge diffusion equates to more WMD incidents by non-state actors.

The limited amount of open source data on CBRN events makes it impossible to rely solely on empirical analysis; therefore, the third chapter also surveys the al-Qaeda organization's WMB pursuits. The al-Qaeda case study in this chapter was chosen because of the rich amount of publicly available information compared to other terrorist groups with similar WMD aspirations. The research concludes that the Internet was pivotal to al-Qaeda propagating a religious justification for WMD attacks, gathering knowledge on WMD, communicating with technical experts, coordinating attack plans, and providing virtual training to would-be jihadists.[6] [7]

However, the allied governments' aggressive counterterrorism responses after the September 11th attacks have quelled al-Qaeda's WMD program, making it apparent that other factors such as a permissive operating environment, freedom of movement, access to skilled technicians, and financial resources are ultimately more

[6] Hoffman, Bruce. RAND, "Congressional Testimony: The Use of the Internet by Islamic Extremists." Last modified May 2006. Accessed June 17, 2013. http://www.rand.org/content/dam/rand/pubs/testimonies/2006/RAND_CT262-1.pdf.

[7] Forest, James, and Sammy Salama. Jihadist Tactics and Targeting. Jihadists and Weapons of Mass Destruction. Edited by Gary Ackerman and Jeremy Tamsett. Boc: CRC Press, 2009.

important in aggregate than the benefits the Internet affords. Conversely, the Internet arguably saved al-Qaeda from extinction through virtual propaganda and proxies, and allows the group – and its CBRN threat – to survive, albeit in a less substantial form.

As previously discussed, the independent variable tested in this thesis is the Internet, but for the purposes of this paper many terms such as ICT, cyberspace, new media, and the fifth domain are used interchangeably. The Internet is a transnational telecommunications system connected by a series of networked computers connected to other networked computers around the world, otherwise known as a "network of networks."[8] [9] Most observers incorrectly equate this definition with the World Wide Web when in fact the Web is just one of the systems used to access the Internet. It is an important distinction since this thesis is not only concerned with the Web but all of the elements that individuals use on the Internet, such a mobile phones, social media, satellite connections, email, instant messaging, and so forth. Traditional media is defined by platforms like radio and television and are not encompassed in the definition of new media for this paper, although they do have important historical contexts.

Finally, "power" is broadly defined as the ability to secure one's political objectives, but this thesis is most interested in testing a narrower definition of power: the degree to which the isolated use of cyber elements allows one to achieve political objectives. For a successful experiment, power differentials (the dependent

[8] "A Virtual Counter-Revolution," *The Economist*, September 4, 2010, 75.
[9] "Internet Basics," Florida Center for Instructional Technology, http://fcit.usf.edu/Internet/chap1/chap1.htm. (accessed November 19, 2010).

variable) must be altered significantly by the independent use of ICT. Events where the outcomes would not be dramatically different with or without the cyber campaign are considered null. As this thesis will detail in the following three chapters, the hypothesis presented above will fail: the use of the Internet in interstate, intrastate and extrastate struggles transformed the experience of warfare in some instances, but it did not significantly alter power differentials in any of the cases analyzed, and did not change the outcome of said conflicts.

CHAPTER 1 – CYBERSPACE AND INTERSTATE CONFLICT: RUSSIAN CASE STUDIES FROM 2007-2008

Every month, U.S. government ICT networks experience approximately 1.8 billion cyber attacks against Congressional and Federal agencies.[10] Industry analysts estimate that cybercrime could cost corporations upwards of one trillion dollars annually in stolen intellectual property and identity datasets.[11] In 2008, the Department of Defense experienced the "most significant breach of U.S. military computers ever" when a foreign intelligence agency placed an infected flash drive onto a classified computer.[12] Undoubtedly, global connectivity facilitated by the Internet has advantageously transformed much of modern life, but it has also generated new and unanticipated vulnerabilities for individuals, industry, and governments.

In the context of warfare, technical experts and theorists are at odds over how exactly cyberspace is impacting nation state competition. While some purport that the Internet simply represents a new tool available to militaries, others contend that it has innate transformative properties that will eventually render others forms of warfare irrelevant. If this is the case, traditional notions of state power must be thoroughly reassessed. This chapter seeks to understand whether the Internet is substantively affecting warfare between nation states, and if so, what the ramifications are for how society perceives warfare and conflict, the very nature and definition of war, and how power is distributed among competing states. This paper

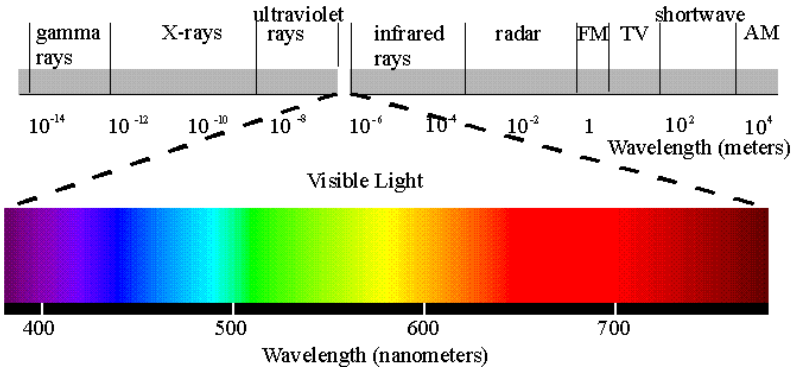
[10] McConnell, Mike. Cyber Insecurities: The 21st Century Threatscape. *America's Cyber Future*, Volume II. CNAS, 2011. https://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume II_2.pdf (accessed September 30, 2013).
[11] Ibid.
[12] "Defending a New Domain." Foreign Affairs. N.p., 1 Sept. 2010. Web. 2 Dec. 2013. http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

will begin with a review of the salient literature on cyber war and the fundamental theories under debate, followed by an examination of two key Russian case studies using a framework for evaluation posited by Eliot Cohen in 1996.

Literature Review

To construct a coherent theoretical framework for cyberspace, one must contextualize the broader "information revolution" from which the Internet's purported transformational properties are derived. Contrary to some assertions,[13] the "fifth domain" is not man-made but rather it is encompassed in the electromagnetic spectrum,[14] [15] which is exploitable because of technological invention. Just as earth's atmosphere was not man-made, human innovation in the form of aircraft allowed for the exploitation of airspace in pursuit of military objectives.

Figure 1.A - The Electromagnetic Spectrum[16]



[13] Nye, Jr., Joseph. *The Future of Power*. New York City: Public Affairs, 2011.
[14] Kuehl, Daniel "The Information Revolution and the Transformation of Warfare," in Karl de Leeuw & Jan Bergstra editors, *The History of Information Security* (Amsterdam, Netherlands: Elsevier, 2007): 823
[15] Hare, Forrest. 2007. "Five Myths of Cyberspace and Cyberpower." SIGNAL Magazine (June). http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=1333&zoneid=209
.
[16] "Electromagnetic Spectrum." http://www.yorku.ca/eye/spectru.htm (accessed November 21, 2010).

While there is considerable debate over whether all or part of the electromagnetic spectrum should be characterized as a new battle space domain, it is clear that a new information environment has emerged, which is "characterized by the use of electronics and the electromagnetic spectrum to create, store, modify and exchange information via networked information systems and infrastructures."[17] According to Daniel Kuehl, this information environment is defined by three elements: connectivity, content and the cognitive.[18] "Connectivity" refers to physical and human connections through technical devices; "content" contains the words, images, and actions that are shared globally through connectivity; and the "cognitive" is the arena of influence and perception. [19]

Though cyber technologies are already having an impact on the realms of military and grand strategy, theorists and practitioners have not agreed upon a unified definition for what constitutes cyber war. Nor have they defined the types of actions in cyberspace that would characterize acts of war and could in turn ignite conflict in the physical world.[20] This is not surprising given the rapidity at which the fifth domain, also known somewhat narrowly as "cyberspace," has developed. Nevertheless, the lack of clear definitions not only muddles the waters of theory, but also creates uncertainty and miscommunication in international affairs.

Historically, military scholars and strategists have struggled to define operational concepts and adapt to new domains in their infancies, affecting both the

[17] Kuehl, Daniel "The Information Revolution and the Transformation of Warfare," in Karl de Leeuw & Jan Bergstra editors, *The History of Information Security* (Amsterdam, Netherlands: Elsevier, 2007): 823
[18] JHU class notes; Fall 2010
[19] JHU class notes; Fall 2010
[20] Mahnken, Thomas. *Cyberwar and Cyber Warfare*. *America's Cyber Future, Volume II*. CNAS, 2011. https://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume II_2.pdf (accessed September 30, 2013).

development of international norms and slowing military reorganization. For example, air power revolutionized war by making conflict three-dimensional.[21] Among other advantages, the advent of air forces altered the nature of reconnaissance missions, since for the first time commanders gained an aerial view behind enemy lines.[22] However, despite air power's outsized role during World War II, including devastating strategic bombing campaigns and delivering a nuclear payload, the U.S. Air Force did not become a separate branch of the U.S. Military until 1947, after the war ended.[23] Additionally, airplanes first crossed international borders to bomb other countries in 1917 during World War I. Yet, it was not until 1926 that international law was agreed upon to declare that a country's sovereign borders existed in the air as well.[24]

Cyberspace is no exception. In 1969 the Defense Department's ARPANET, the precursor to the modern Internet, began a "rudimentary" exchange of digital packets of information between computers. By the early 1980s, the first computer viruses were created.[25] In 1989 the World Wide Web was launched; the prolific search engine, Google, debuted in 1998.[26] Yet, it was not until 2009 that the U.S. Secretary of Defense authorized the creation of the United States Cyber Command (USCYBERCOM), which was finally fully operational on October 31,

[21] Dr. Tami Biddle (Fall 2009); speech at Johns Hopkins University.
[22] Ibid.
[23] http://www.af.mil/information/factsheets/factsheet.asp?id=2 (accessed 1 December 2010)
[24] JHU class notes; Fall 2010
[25] Nye, Jr., Joseph. *Cyber Power*. Manuscript, Harvard Kennedy School, 2010. http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.
[26] Ibid. 3

2010.[27] Problems persisted, since USCYBERCOM was mandated with protecting the Defense Department's .mil networks only, whereas 90 percent of the American Internet system is civilian and no U.S. government agency has "line responsibility" for securing those networks.[28] The United States government has therefore required over four decades to only begin adapting to its own invention.

Schools of Thought

Because cyberspace is a relatively new area for conflict, scholarship on cyber conflict has been fragmentary, often focusing heavily on the technicalities of networks, or alarmist predictions, such as a "cyber Pearl Harbor,"[29] not rooted soundly in empirics.[30] Hans-Igne Langø argues that there is "…little common understanding of the conceptual and theoretical nature of cyberspace as it relates to security," complicating a systematic evaluation of cyber's effects on war and power dynamics. [31]

Langø has categorized the nascent schools of thought on cyber security into three groups: Revolutionist, Traditionalist, and Environmentalist.[32] In Langø's view, the "Revolutionist" thinkers believe that the Internet can greatly alter armed conflict, asserting that the latent revolutionary characteristics of the fifth domain

[27] "Fact Sheet." *U.S. Cyber Command* (blog), August, 2013. http://www.stratcom.mil/factsheets/Cyber_Command/ (accessed November 3, 2013).
[28] McGraw, Gary, and Nathaniel Fick. *Separating Threat from the Hype: What Washington Needs to Know about Cyber Security*. *America's Cyber Future, Volume II*. CNAS, 2011. https://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume II_2.pdf (accessed September 30, 2013).
[29] McConnell, Mike. *Cyber Insecurities: The 21st Century Threatscape*. *America's Cyber Future, Volume II*. CNAS, 2011. https://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume II_2.pdf (accessed September 30, 2013).
[30] Langø, Hans-Inge. *Slaying Cyber Dragons: Competing Approaches to Cyber Security*. Working paper, Norwegian Institute of International Affairs, 2013.
[31] Ibid. 5
[32] Ibid. 5

are transforming the very nature of war.[33] Conversely, "Traditionalist" thought rejects the notion that the nature of war is being transformed by the information revolution, contending instead that information technology will not upend the normal order in international relations.[34]

Langø's third cyber security group, the "Environmentalist" thinkers, is the newest and least cogent of the three groups. They assert that traditional international relations theory does not translate easily into cyber security discussions due to the Internet's "unique nature." [35] Environmentalists are essentially Revolutionists in scope but prefer to emphasize the Internet's non-violent properties and power transference, while trying to deflect away from the Internet's role in warfare. It should also be noted that Langø's three classifications – Revolutionist, Traditionalist, and Environmentalist – are generalized groupings and major variations in opinion exist within each category.

The following will utilize Langø's cyber security classification framework to analyze three key deliberations in current cyber war scholarship, ranging from the philosophical to the practical. These points of contention were plucked from the existing literature in order to compare and contrast the "competing approaches" to cyber security of which this author believes are the essential arguments framing the current debate.

[33] Ibid. 9
[34] Ibid. 19
[35] Langø, Hans-Inge. *Slaying Cyber Dragons: Competing Approaches to Cyber Security*. Working paper, Norwegian Institute of International Affairs, 2013.

What is Cyber War?

Prussian Military strategist Carl von Clausewitz famously theorized, "…war is simply a continuation of political intercourse, with the addition of other means."[36] Traditionalist Thomas Rid describes Clausewitz's three criteria that must be fulfilled for actions to be considered acts of war: violence or potential violence; the threat of force to compel an adversary; and an articulable political objective.[37] The fundamental question in cyber conflict is this: can cyber war exist without physical (or political) violence or attribution to achieve one's desired political ends? Thomas Rid argues it cannot, and that not a single cyber attack to date has fulfilled all of Clausewitz's definition of war.[38]

While fellow Traditionalist Thomas Mahnken agrees that cyber war (which he defines as the independent use of the cyber instrument to achieve strategic objectives) has yet not occurred, he does not dismiss its potential. Rather, Mahnken argues that some instances of cyber warfare have occurred when nation states employed cyber tools as a force multiplier in larger military conflicts.[39] Thus, in his view, cyber war is unlikely to be decisive on its own, but "cyber warfare in support of other military instruments is likely to be an increasingly prevalent form of combat."[40]

Environmentalists Greg McGraw and Nathaniel Fick provide their own view on cyber war claiming that cyber war must have a kinetic or "consequential impact

[36] Clausewitz, Carl von. *On War*. Radford, VA: Wilder Publications, LLC, 2008.
[37] Rid, Thomas. 2013. Cyberwar and peace. *Foreign Affairs* 92 (6) (11/01): 77.
[38] Ibid.
[39] Mahnken, Thomas. *Cyberwar and Cyber Warfare*. *America's Cyber Future, Volume II*. CNAS, 2011. https://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume II_2.pdf (accessed September 30, 2013).
[40] Ibid. 58

in the physical world."[41] This contrasts with Mahnken's view, as his framework requires that an act of cyber war not cross into the physical world. McGraw and Fick present a hypothetical scenario where an adversary infects the opposing state's command and control systems for Unmanned Combat Aerial Systems, causing them to launch weapons at the wrong targets. This, they argue, would constitute an act of cyber war; whereas this scenario seems to fit Mahnken's view of cyber warfare, because the cyber act is enabling the physical domains for kinetic action. [42]

The definitional discrepancies do not end there. While one could dismiss these differences as parsing of phrases, the lack of an established concept on cyber war has stymied efforts to analyze the cyber domain, establish international norms, and reorganize national security bureaucracies. These discrepancies in definition are unlikely to be resolved easily, because they drive to the core of the strength of the cyber domain: as Kuehl elaborates, the fifth domain technically exists in both physical and virtual worlds, and is not confined to geographic boundaries. [43] This renders the definition of dimensions a lofty task, perhaps explaining the glacial pace at which the U.S. government has adapted to developments in this domain since the 1970s. Of note, Revolutionist contributions to the cyber war definition debate is a far more expansive topic which must be summarized in the context of the cyber's impact on the nature of warfare itself.

---

[41] McGraw, Gary, and Nathaniel Fick. *Separating Threat from the Hype: What Washington Needs to Know about Cyber Security*. *America's Cyber Future, Volume II*. CNAS, 2011. https://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume II_2.pdf (accessed September 30, 2013).

[42] Mahnken, Thomas. *Cyberwar and Cyber Warfare*. *America's Cyber Future, Volume II*. CNAS, 2011. https://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume II_2.pdf (accessed September 30, 2013).

[43] Kuehl, Daniel "The Information Revolution and the Transformation of Warfare," in Karl de Leeuw & Jan Bergstra editors, *The History of Information Security* (Amsterdam, Netherlands: Elsevier, 2007): 823.

Nature of War

What is described today as the Revolutionist school of thought on cyber war is rooted in the "revolution in military affairs" (RMA) theories that were first articulated over three decades ago.[44] Eliot Cohen, writing in the mid-1990s, described RMA's beginnings in the 1980s when Soviet strategists, such as the chief of the general staff Marshal Nikolai Ogarkov, promulgated notions of an "imminent technical revolution."[45] American theorists were evaluating ICT's influence on warfare as early as 1976, when defense analyst Thomas P. Rona "coined the term 'information warfare' in a report on the potential vulnerabilities of U.S. weapons platforms that had become reliant on computer systems."[46] Early Revolutionist theorists John Arquilla and David Ronfeldt argued that future warfare would be determined by competition in effectively collecting and exploiting battlefield intelligence, and rather than simply deploying the most capital, labor, and technology onto the battlefield.[47]

The period after the first Gulf War, when the technologically superior U.S. military crushed an Iraqi military with a half million troops who were equipped with relatively advanced Soviet weaponry, further fueled the RMA speculations. Andrew Krepinevich in 1994 posited that American military operations in that Gulf War did not meet the historical criteria for RMA, but strongly suggested the United

[44] McNaugher, Thomas L. 2007. The real meaning of military transformation: Rethinking the revolution: Review essay. Foreign Affairs 86 (1) (01/01): 140.
[45] Cohen, Eliot A. 1996. A revolution in warfare. Foreign Affairs 75 (03/01): 37.
[46] Langø, Hans-Inge. *Slaying Cyber Dragons: Competing Approaches to Cyber Security*. Working paper, Norwegian Institute of International Affairs, 2013.
[47] Arquilla, John, and David Ronfeldt. "Cyberwar is Coming!" *Comparative Strategy* 12, no. 2 (1993): 141-165.

States military was on the precipice of revolutionary change.[48] Arguments such as these spawned even more terms like "network-centric warfare" (or "netwar"), Strategic Information Warfare (SIW), and Computer Network Operations (CNO), among others. Some contend that this line of thinking arguably influenced U.S. Defense Secretary Donald Rumsfeld's decision to dedicate relatively few forces during the Second Gulf War.[49] [50] Traditionalists, like Fredrick Kagan, criticized these experimental warfare theories as "exotic" and "increasingly divorced from reality"[51] since they emphasized collapsing the enemy through technological superiority, while ignoring the Clauswitzian need to construct a positive political end-state after combat operations, which he believes hampered the second American mission in Iraq. [52]

Today, contemporary Revolutionists like Robert Miller and Kuehl postulate that technological achievements in communications from Gutenberg's printing press to wireless Internet have produced an "omniconnected" world, giving birth to a revolution in military affairs, which is transforming warfare through a new operational medium: cyberspace.[53] Some modern Revolutionists, having suffered somewhat of a defeat of their ideas in the Second Gulf War when primitive insurgents stymied the technologically superior coalition forces, have adjusted their theories. They now argue that in the 21st century, cyberspace is emerging as the

---

[48] Krepinevich, Andrew F. *Cavalry to Computer: The Pattern of Military Revolutions*. National Affairs, 1994.
[49] Langø, Hans-Inge. *Slaying Cyber Dragons: Competing Approaches to Cyber Security*. Working paper. Norwegian Institute of International Affairs, 2013.
[50] McNaugher, Thomas L. 2007. The real meaning of military transformation: Rethinking the revolution: Review essay. Foreign Affairs 86 (1) (01/01): 140.
[51] Ibid.
[52] Ibid.
[53] Miller, Robert A., and Daniel T. Kuehl. *Cyberspace and the 'First Battle' in 21st-century War*. Center for Technology and National Security Policy, National Defense University, 2009: 821, 822

decisive battlespace where the victors of strategic conflicts will ultimately be determined.[54] [55] The popular focus is now less on information dominance in the battlefield (although some remain vocally supportive of that notion) and more about how the cyber domain is changing the nature of war by supplanting established conflict domains, an effect which they believe has the potential to overturn the existing world order.[56]

Traditionalists fervently disagree. Mahnken critiques the cyber Revolutionists on their fundamental point; he contends that they have failed to articulate a casual theory for how exactly the independent use of cyber war will achieve political ends in a manner that supersedes the relevance of other domains.[57] In fact, Erik Gartzke contends that many of the real-world examples of cyber acts that Revolutionists use to underpin their claims are more appropriately defined as cyber espionage, cyber sabotage, or cybercrime.[58] He argues that some cyber acts are merely an augment to traditional military actions, and what many call cyber war is really just an "…adjunct to, rather than a substitute for, existing forms of political violence."[59]

---

54 Ibid.
55 Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38, no. 2 (2013): 41-73.
56 Ibid.
57 Mahnken, Thomas. *Cyberwar and Cyber Warfare*. *America's Cyber Future, Volume II*. CNAS, 2011. https://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume II_2.pdf (accessed September 30, 2013).
58 Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38, no. 2 (2013): 41-73.
59 Ibid.

Power Diffusion

Both Revolutionists and Environmentalists accept that ICT "erodes hierarchies, collapses time and distance, and empowers networks,"[60] thereby deteriorating traditional power structures and creating new vulnerabilities for larger states.[61] While Revolutionists and Traditionalists have conflicting views on the cyber domain's importance in military affairs, Environmentalists have adopted the Revolutionist opinion of the Internet's inherent transformative properties and applied it to a loosely defined concept of "cyber power."[62] They define of cyber power as "the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power."[63]

The principal argument of Joseph Nye, a leading Environmentalist thinker, is that a great political shift is underway in which power is diffused from governments to individuals, and will eventually create a "non-polar" world.[64] While positing an intriguing theory, Nye comes up short in providing empirical data to support his Environmentalist thesis, mainly because he is portending how the world could appear many decades from now. Nye acknowledges that governments are the most powerful actors at present, and he envisions a future where nation states are less important in individuals' lives in part because cyberspace reduces "power

---

[60] Segal, Adam. "What to Read on Cybersecurity." *Foreign Affairs* (blog), November 12, 2012. http://www.foreignaffairs.com/features/readinglists/what-to-read-on-cybersecurity (accessed October 6, 2013).

[61] Nye, Jr., Joseph. *The Future of Power*. New York City: Public Affairs, 2011.

[62] Ibid.

[63] Nye, Jr., Joseph. *Cyber Power*. Manuscript, Harvard Kennedy School, 2010. http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

[64] Nye, Jr., Joseph. Harvard Belfer Center, "Cyber War and Peace." Last modified April 10, 2012. Accessed October 6, 2013. http://belfercenter.ksg.harvard.edu/publication/21937/cyber_war_and_peace.html?breadcrumb=/project/67/explorations_in_cyber_international_relations.

differentials among actors"[65] since the "barriers to entry in the cyber domain are so low that non-state actors and small states can play a significant role at low cost."[66]

Some pessimists within the Revolutionist camp agree with Nye's Evolutionist theory, but view this as a strategic vulnerability that could lead to a cyber Pearl Harbor unless nation states are quick to properly defend against said vulnerabilities. Thus some Revolutionists propose top-down, whole of government solutions like a national cyber security center modeled after the National Counterterrorism Center (NCTC), as proposed by the former Director of National Intelligence (DNI), Mike McConnell.[67]

Traditionalist Sean Lawson provides an alternative perspective on pessimistic Revolutionists who postulate "cyber-doom scenarios,"[68] such as an attack akin to a "cyber 9/11."[69] By utilizing scholarship from disaster sociology, military history, and the history of technology, Lawson asserts that much of the present cyber-doom hypotheticals are rooted in technological determinism.[70] He describes this as the "'feeling that our collective life in society is uncontrollable' as a result of our increasing dependence on technology."[71] Present day technological determinism is not an anomaly; Lawson draws a corollary to public reaction to the telegraph in the early 20th century: the then-new transcontinental communication

---

[65] Ibid.
[66] Ibid.
[67] McConnell, Mike. *Cyber Insecurities: The 21st Century Threatscape*. *America's Cyber Future, Volume II*. CNAS, 2011. https://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume II_2.pdf (accessed September 30, 2013).
[68] Lawson, Sean. "Beyond cyber-doom: Cyberattack Scenarios and the Evidence of History." *Mercatus Center George Mason University Working Paper* 11-01 (2011).
[69] Ibid.
[70] Ibid.
[71] Ibid.

network the media described as a "new space" gave rise to the fear that "wire devils" – perhaps analogous to computer hackers – could use the telegraph to crash the entire U.S. economy.[72]

Additionally, one must be note that Traditionalist thinkers are directly opposed to the Environmentalist and Revolutionist belief that the Internet provides a comparative advantage to weaker states under the auspices of war. Nye states that large state powers will be unable to achieve dominance in the cyber domain as they have in the air, land, and sea, though they will continue to exercise exclusivity on the use of force in the physical world.[73] [74] Mahnken and Gartzke counter this thesis by arguing that cyber cannot "compensate for weakness in other instruments of power,"[75] and that cyber war "appears much more likely to augment the military advantages of status quo powers."[76]

As evidence, they cite the limited ability of states to use the Internet to coerce or compel a desired political outcome, unlike traditional military violence.[77] Gartzke in particular cannot conceive of a need for a powerful state to dominate the cyber domain, since "cyber attacks are unlikely to prove particularly potent in grand

---

[72] Ibid.

[73] Nye, Jr., Joseph. Harvard Belfer Center, "Cyber War and Peace." Last modified April 10, 2012. Accessed October 6, 2013. http://belfercenter.ksg.harvard.edu/publication/21937/cyber_war_and_peace.html?breadcrumb=/project/67/explorations_in_cyber_international_relations.

[74] Nye, Jr., Joseph. *The Future of Power*. New York City: Public Affairs, 2011.

[75] Mahnken, Thomas. *Cyberwar and Cyber Warfare*. *America's Cyber Future, Volume II*. CNAS, 2011. https://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume II_2.pdf (accessed September 30, 2013).

[76] Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38, no. 2 (2013): 41-73.

[77] Ibid.

strategic terms unless they are accompanied by terrestrial military force."[78] Mahnken concurs, noting that a cyber attack against a state's economic infrastructure is highly unlikely to produce more damage than an air raid.[79] Even those who promote preparation for cyber doom admit that there has yet to be a cyber attack against critical infrastructure of any consequence.[80] However, the absence of evidence is not evidence of absence, and it remains to be seen if a catastrophic cyber attack will occur, and if so, how states should prepare themselves.

In the end, all schools of thought are wanting in some fashion. Many Traditionalists are correct to focus on the continuing importance of the physical realm in military affairs and appear to have the greatest explanatory value in the present, but are perhaps overly dismissive of the possibilities of information technology in the future. Conversely, many Revolutionists and Environmentalists are open to those very future possibilities, but are overstate the present applicability of information technology to international affairs.

Case Studies

Many current cyber war studies fail to systematically evaluate key cyber attacks in the context of broader geostrategic contests, which could offer more sounds judgments on how the fifth domain is impacting nation state competition.

---

[78] Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38, no. 2 (2013): 41-73.

[79] Mahnken, Thomas. *Cyberwar and Cyber Warfare*. *America's Cyber Future, Volume II*. CNAS, 2011. https://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume II_2.pdf (accessed September 30, 2013).

[80] McConnell, Mike. *Cyber Insecurities: The 21st Century Threatscape*. *America's Cyber Future, Volume II*. CNAS, 2011. https://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume II_2.pdf (accessed September 30, 2013).

The following section of the paper seeks to correct that by using a theoretical framework to examine the evidence on two pivotal cyber events, thereby offering a contribution to the academic debate on the Internet's impact on war. The scope of these case studies are limited to interstate cyber struggles in the context of warfare as surveying every element in cyber conflict, ranging from criminality to espionage, would be far too expansive a topic. Additionally, these case studies were selected because they represent two instances of interstate conflict with sizeable cyber components, both of which have been analyzed in depth in academia and security professionals.

The first case study focuses on Russia's 2007 conflict with Estonia. This conflict occurred almost entirely in the realm of cyberspace, which allows one to evaluate the particular utility of the cyber component as a tool for political coercion. Conversely, the second case study will investigate Russia's 2008 clash with Georgia, which took place in both the physical and cyber domains. This case study will enable analysis of the cyber component's function in a wider interstate conflict.

To evaluate the Internet's role as a transformative technology, this paper will rely on a framework first elucidated by Eliot Cohen in 1996. Cohen posited four questions to evaluate whether the world was on the precipice of an information-led revolution in military affairs: "Will it change the appearance of combat? Will it change the structure of armies? Will it lead to the rise of new military elites? Will it alter countries' power position?"[81] This framework, more so than others on the subject of military revolutions, affords the ability to analyze and weigh the

[81] Cohen, Eliot A. 1996. A revolution in warfare. Foreign Affairs 75 (03/01).

significance of a number of new military technologies across a range of cultures and time. This paper will apply these questions more narrowly to the Internet and gauge how two Russian cyber warfare case studies measure up to Cohen's 17-year-old thesis.

Russia and Estonia

The 2007 conflict between Russia and Estonia marked a consequential inflection point in the study of cyber security, as it was contested solely in the fifth domain. Estonia is a small but hyper-connected society that is highly dependent on the Internet for routine functions of the state and commerce.[82] Tensions between Russia and Estonia dated to the Soviet Union's 1940 annexation of the Baltic States, which Russia views as the Red Army's liberation of the Baltics from Nazi forces in World War II.[83] The Soviets memorialized that sacrifice with a bronze statue of a Red Army soldier in Estonia's capital of Tallinn, as they did in many other state capitols in the Soviet sphere of influence.[84]

During WWII and throughout the Cold War, the Kremlin sought to "Russify" Eastern bloc countries and conducted a mass migration of ethnic Russians to Estonia, intensifying ethnic tensions, an agitation that still exists today.[85] For the minority of ethnic Russians living in Estonia, the bronze solider in Tallinn is a "cherished memorial of wartime sacrifice," especially since it is ensconced in the

[82] Clarke, Richard A., and Robert Knake. *Cyber War: The next threat to national security and what to do about it*. HarperCollins, 2010: 12.
[83] Herzog, Stephen. 2011. Revisiting the Estonian cyber attacks: Digital threats and multinational responses. Journal of Strategic Security 4 (2) (05/01): 50.

[85] Ibid. 50
[85] Ibid. 50

graves of Russian veterans, making the site sacred to many. However, native Estonians view it as a "symbol of a hated occupation."[86]

The tensions reached a boiling point in February 2007 when the Estonian legislature, representing the majority popular opinion, voted to take down the large bronze solider to rid the city center of the giant reminder of repression.[87] The Estonian President vetoed the law to avoid inciting riots; however, on April 27, 2007, ethnic Russians and Estonians protesting at the site clashed. The situation quickly devolved into rioting and looting.[88] [89]

To save the statue from the violence, the Estonian government moved it from the city's center to the Tallinn Military Cemetery, a less visible location that Russian-speaking minority viewed as representing a marginalization of their ethnic identity.[90] This move failed to have its desired effect, instead igniting a nationalist response in Russia's media and legislature.[91] Protests spread to Moscow, and enraged activists blockaded the Estonian Embassy.[92]

Provocations from ethnic and nationalist disputes are not unusual, but the cyber components, which accompanied the riots in this case study, were unique for the time. As the protests turned violent, a month-long cyber assault commenced,

---

[86] A cyber-riot. 2007. Economist 383 (8528) (05/12): 55.
[87] Clarke, Richard A., and Robert Knake. *Cyber War: The next threat to national security and what to do about it*. HarperCollins, 2010: 12.
[88] A cyber-riot. 2007. Economist 383 (8528) (05/12): 55.
[89] Clarke, Richard A., and Robert Knake. *Cyber War: The next threat to national security and what to do about it*. HarperCollins, 2010: 13.
[90] Herzog, Stephen. 2011. Revisiting the Estonian cyber attacks: Digital threats and multinational responses. Journal of Strategic Security 4 (2) (05/01): 51.
[91] Clarke, Richard A., and Robert Knake. *Cyber War: The next threat to national security and what to do about it*. HarperCollins, 2010: 13.
[92] Silverman, Jacob. "Could hackers devastate the U.S. economy?" *How Stuff Works* (blog), http://computer.howstuffworks.com/die-hard-hacker1.htm (accessed November 2, 2013).

crippling Estonian government and financial websites, halting online banking, newspaper websites, and electronic government services for days.[93] In Estonia, 97 percent of bank transactions are virtual, and even the water supply is dependent on the Internet, along with other critical infrastructure. These factors made the cyber attacks acutely uncomfortable for Estonia's citizens.[94] Distributed denial of service (DDoS) attacks[95] were the hallmark of the cyber campaign against Estonia, but hackers also disabled the Parliament's e-mail server for a short time, defaced many websites, and posted a fake letter of apology from the Prime Minister on the Reform Party's website.[96] [97]

The distributed nature of the Russian DDoS attack against Estonia refers to the thousands or possibly hundreds of thousands of "zombie" computers, also known as "botnets,"[98] that in a coordinated manner simultaneously requested information from a targeted website. This flood of data overwhelmed the servers, switches, and routers and crashed chosen websites, making it impossible for legitimate actors to gain access.[99][100] This technique can also be called "swarming"

[93] Landler, Mark, and John Markoff. "Digital Fears Emerge After Data Siege in Estonia." New York Times, May 29, 2007. http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0 (accessed September 26, 2013).

[94] Herzog, Stephen. 2011. Revisiting the Estonian cyber attacks: Digital threats and multinational responses. Journal of Strategic Security 4 (2) (05/01): 51.

[95] According to Richard Clarke, DDoS attacks are a "preprogrammed flood of Internet traffic designed to crash or jam networks."

[96] Landler, Mark, and John Markoff. "Digital Fears Emerge After Data Siege in Estonia." New York Times, May 29, 2007. http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0 (accessed September 26, 2013).

[97] A cyber-riot. 2007. Economist 383 (8528) (05/12): 55.

[98] According to Symantec, "A 'bot' is a type of malware that allows an attacker to take control over an affected computer. Also known as 'Web robot'", bots are usually part of a network of infected machines, known as a 'botnet', which is typically made up of victim machines that stretch across the globe." http://us.norton.com/botnet/

[99] Clarke, Richard A., and Robert Knake. *Cyber War: The next threat to national security and what to do about it*. HarperCollins, 2010: 14.

and is organized by hackers who hijack or even rent zombie computers to orchestrate an attack.[101] In the case of Estonia, a government website that routinely averaged 1,000 visitors daily suddenly had 2,000 data requests per second.[102]

Government officials in Tallinn concluded they were experiencing Russian state-sponsored cyber terrorism, claiming the Internet address of one the computers participating in the attacks was traced to a Russian government official working for President Vladimir Putin.[103] Moscow claimed the acts were solely the product of "patriotic hackers" and denied any government involvement.[104] [105] Subsequent North Atlantic Treaty Organization (NATO) and European Commission inquiries could not find definitive evidence linking the cyber attacks to the Kremlin.[106] Although one NATO official suggested state involvement: "…these were not things done by a few individuals. This clearly bore the hallmarks of something concerted."[107]

Circumstantial evidence was plentiful in open source investigations; the Russian government did not cooperate with the Estonians to track down the cyber perpetrators, instead inciting greater tensions by calling the Estonians "fascists,"

---

[100] Franklin, Curt. "How Routers Work." *How Stuff Works* (blog), http://computer.howstuffworks.com/router11.htm (accessed November 2, 2013).
[101] Herzog, Stephen. 2011. Revisiting the Estonian cyber attacks: Digital threats and multinational responses. Journal of Strategic Security 4 (2) (05/01): 52.
[102] Ibid. 52
[103] Landler, Mark, and John Markoff. "Digital Fears Emerge After Data Siege in Estonia." *New York Times*, May 29, 2007. http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0 (accessed September 26, 2013).
[104] Silverman, Jacob. "Could hackers devastate the U.S. economy?" *How Stuff Works* (blog), http://computer.howstuffworks.com/die-hard-hacker1.htm (accessed November 2, 2013).
[105] Pitcairn, Daniel. "A Missed Chance for NATO's Cybersecurity Future." *Defense One*, October 23, 2013. http://www.defenseone.com/ideas/2013/10/missed-chance-natos-cybersecurity-future/72542/?oref=d-interstitial-continue (accessed October 30, 2013).
[106] Herzog, Stephen. 2011. Revisiting the Estonian cyber attacks: Digital threats and multinational responses. Journal of Strategic Security 4 (2) (05/01): 51
[107] Ibid. 51

and chose not to do anything as protestors blockaded the Estonian Embassy in Moscow.[108] [109] It was not until NATO and the European Union belatedly expressed outrage that the Russians begrudgingly agreed to a deal brokered by Germany, and the blockade abruptly ended,[110] suggesting Moscow did in fact have a measure of control over the protestors. Cyber experts also speculate about the likelihood of state government collusion, noting the sophistication of what at that time was considered a highly complex attack, and that it was well financed using rented botnets.[111] University of Southern California's Douglas Thomas explained, "99 percent of…hackers do not have the skill or the ability to organize or execute an attack that would be anything more than a minor inconvenience."[112]

GreyLogic, an open source cyber intelligence consulting service for governments, undertook in-depth analysis of the Russian military's Information Warfare (IW) doctrine and the cyber attacks on Estonia in 2007 and Georgia in 2008.[113] Even before the physical skirmishes began in late April 2007, "hacktivists" in Russian-language chat rooms and other web forums posted descriptive information on how to participate in DDoS attacks, and which Estonian websites to

[108] Ibid. 51
[109] Landler, Mark, and John Markoff. "Digital Fears Emerge After Data Siege in Estonia." *New York Times*, May 29, 2007. http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0 (accessed September 26, 2013).
[110] A cyber-riot. 2007. Economist 383 (8528) (05/12): 55.
[111] Landler, Mark, and John Markoff. "Digital Fears Emerge After Data Siege in Estonia." *New York Times*, May 29, 2007. http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0 (accessed September 26, 2013).
[112] Herzog, Stephen. 2011. Revisiting the Estonian cyber attacks: Digital threats and multinational responses. Journal of Strategic Security 4 (2) (05/01): 49.
[113] Carr, Jeffrey. 2009. *The Evolving State of Cyber Warfare*. Phase 2. Project Grey Goose. http://fserror.com/pdf/GreyGoose2.pdf

target.[114] GreyLogic's analysis concluded that the Russian military has acknowledged utilizing cyber attacks that appear to be cyber terrorism or cybercrime has strategic value and creates plausible deniability.[115] In the case of Estonia, the Russian *Nashi* youth movement,[116] funded in part by the Kremlin, participated in the protests against the Estonian Embassy in Moscow and allegedly in the Estonia DDoS attacks.[117]

Despite the lack of a smoking gun, it seems clear that the Russian government decided to at least passively support (and most likely, actively sponsor) interstate cyber-terrorism to gain political leverage over Estonia. However, in this case, Russia failed to achieve its political objectives: leadership in Tallinn defied Moscow and moved the sacred statue to a less visible location, where it remains today. Further, the cyber barrage against Estonia's critical economic and government websites served to alert NATO countries to their own cyber vulnerabilities. In 2008 NATO established the Cooperative Cyber Defense Center of Excellence (CCDCOE) in Tallinn to increase cooperation on cyber defense between NATO member nations.[118] In many ways, the cyber attacks against Estonia actually allied them closer with NATO and may have served to decrease Russian political influence in Estonia.

---

[114] Landler, Mark, and John Markoff. "Digital Fears Emerge After Data Siege in Estonia." *New York Times*, May 29, 2007. http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0 (accessed September 26, 2013).

[115] Carr, Jeffrey. 2009. *The Evolving State of Cyber Warfare*. Phase 2. Project Grey Goose. http://fserror.com/pdf/GreyGoose2.pdf

[116] "Nashi (http://nashi.su) is short for *Molodezhnoye demokraticheskoye antifashistskoye dvizhenye* "Nashi" (translation, Youth Democratic Anti-Fascist Movement Ours!)"

[117] Carr, Jeffrey. 2009. *The Evolving State of Cyber Warfare*. Phase 2. Project Grey Goose. http://fserror.com/pdf/GreyGoose2.pdfCarr

[118] *NATO Cooperative Cyber Defense Centre of Excellence*, https://www.ccdcoe.org/ (accessed November 6, 2013).

Russia and Georgia

One year after its clash with Estonia, Russia was embroiled in another cyber conflict with a satellite state, Georgia. This time, the confrontation was also executed in the air, land, and sea domains.[119] Cyber security experts contend the short war "represents the first instance of a large-scale computer network attack (CNA) conducted in tandem with major ground combat operations,"[120] making it ideal to investigate cyber's ability to enhance traditional arenas of warfare in a physical confrontation. As was the case with Estonia, the Kremlin denied involvement in the offensive cyber campaign, but former Director of National Intelligence Mike McConnell, as well as many other security experts, assessed that the assault as consistent with the Russian military doctrine of using cyber weapons as a force multiplier alongside other military capabilities.[121]

The small nation of Georgia has a population of four million and is slightly smaller in size than South Carolina.[122] Georgia originally declared independence from the Russian Empire in 1918 after the Russian Revolution was underway, but once the Red Army was victorious, they recaptured Georgia, installed a puppet government, and brought it into the Union of Soviet Socialist Republics (USSR).[123] After the fall of the Soviet Union, Georgia once again declared independence in 1991, but by 1993 it had lost control of two breakaway territories, South Ossetia and

[119] Shachtman, Noah. "http://www.wired.com/dangerroom/2009/03/georgia-blames/" *WIRED*, March 11, 2009. http://www.wired.com/dangerroom/2009/03/georgia-blames/ (accessed October 15, 2013).
[120] Shakarian, Paulo. "The 2008 Russian Cyber Campaign against Georgia." *Military Review-English Edition* 91, no. 6 (2011): 63.
[121] McConnell, Mike. *Cyber Insecurities: The 21st Century Threatscape*. *America's Cyber Future, Volume II*. CNAS, 2011. https://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume II_2.pdf (accessed September 30, 2013).
[122] Clarke, Richard A., and Robert Knake. *Cyber War: The next threat to national security and what to do about it*. HarperCollins, 2010: 17
[123] Ibid. 17

Abkhazia, in a conflict between Georgian troops and Russian-backed rebels.[124] The disputed territories established independent governments but were not internationally recognized.

Georgia's 2003 "Rose Revolution" changed the country's trajectory away from a post-Soviet kleptocracy towards what many protestors and international observers believed was meaningful political and economic reform.[125] A series on non-violent protests in the capital of Tbilisi forced the president and his party to resign, paving the way for democratic reform under Mikhail Saakashvili and his New National Movement."[126]

Saakashvili had more in mind for Georgia than just economic reforms: he desired to spur Georgia towards integration with the West, including membership in NATO and the European Union. To that end, Saakashvili sent Georgian troops to fight in both the Afghanistan and Iraq war.[127] While Georgia failed in its bid for NATO membership,[128] Moscow took Tbilisi's overtures to the West as an affront. The Kremlin was further antagonized by Saakashvili's public efforts to unify Georgia and gain central control over the disputed territories of South Ossetia, Abkhazia, and Ach'ara.[129] Throughout Saakashvili's Presidency there would be intermittent clashes between the Georgians and Russian-supported ethnic groups in the territories.

---

[124] Ibid. 17,18
[125] Fairbanks, Charles H. "Georgia's Rose Revolution." *Journal of Democracy* 15, no. 2 (2004): 110-124.
[126] Ibid.
[127] Schmitt, Gary. "The Forgotten War." *AEI Ideas* (blog), August 07, 2013. http://www.aei-ideas.org/2013/08/the-forgotten-war/ (accessed November 7, 2013).
[128] As of this writing (fall 2013), Georgia is still seeking NATO membership, a new president was elected, and some of Saakashvili's supporters have been arrested on charges of political corruption and abuse of power.
[129] The Harriman Institute, "Columbia University." Accessed November 7, 2013. http://www.columbia.edu/cu/news/global/images/Post-SovietTimeline.pdf.

Figure 1.B – Timeline of Events Leading to the Five-Day War [130] [131]

Early April 2008	**Georgian membership rejected at NATO Summit.**
16 April 2008	**Russia unilaterally authorizes official relations with Abkhazia and South Ossetia.**
April 2008	**Russia dispatches reinforcement troops to Abkhazia, reportedly in response to increased Georgian aggression.**
3 July 2008	**Tskhinvali shelled, killing three. Convoy carrying Georgian backed South Ossetian interim head of government attacked.**
July 2008	**Russian fighter jets fly over South Ossetia. Georgia withdraws its ambassador from Moscow in response to the violation of its airspace.**
15 July 2008	**8,000 Russian troops train for peace enforcement operations on Georgia's frontier.**
1-2 August 2008	**Georgia claimed a terrorist attack left 5 policemen wounded. Georgia claimed that terrorist attacks hit a peacekeeping battalion and police checkpoint areas.**
7 August 2008	**Georgian forces penetrate South Ossetian capital of Tskhinvali in an effort to retake the city. Russia sends in its own forces, stating it will protect its citizens from Georgian aggression.**

As Figure 1.B depicts, it did not require much expertise to understand that tensions between Russian and Georgia were at an all-time high. In July 2008, Ossetian rebels (probably backed by Moscow) conducted missile raids on Georgian villages, and in turn Georgia bombed Tskhinvali, the capital of South Ossetia.[132] On the night of August 7th, the Georgian Army invaded Tskhinvali to disrupt the rebels and recapture control of their territory in response to alleged Russian provocations.[133] Russia responded by deploying more combat troops to South Ossetia, bombarding the territories and military targets inside Tbilisi with air and artillery strikes, enacting a naval blockade of Georgia, and occupying sovereign

[130] Ibid.
[131] The American Enterprise Institute, "The War in the Caucasus: An Initial Assessment." Last modified August 13, 2008. Accessed November 7, 2013. http://www.aei.org/files/2008/08/13/20080813_PowerpointPresentation.pdf.
[132] Clarke, Richard A., and Robert Knake. *Cyber War: The next threat to national security and what to do about it*. HarperCollins, 2010: 18
[133] Hollis, David. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal*. http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008 (accessed October 15, 2013).

Georgian territory that was never contested.[134] [135] In five days, Russian forces essentially defeated the Georgian military. One military analyst explained: "There has been no parallel to this military operation since Saddam Hussein invaded Kuwait in 1990."[136]

While Russia has a long history of militarily crushing weaker satellite states, this conflict was noteworthy because of the novel cyber attacks that accompanied kinetic operations. As in Estonia, the Kremlin consistently denied collusion in these attacks. However, one prominent cyber security organization assessed that the cyber attacks bore the hallmarks of coordination with the Russian government, if not state sponsorship: "the primary objective of the cyber campaign was to support the Russian invasion of Georgia, and the cyber attacks fits neatly into the invasion plan."[137] In a familiar pattern similar to Estonia, the opening cyber assault consisted of botnets implementing *brute force* DDoS attacks against Georgian government and media websites, shutting down 11 targeted websites.[138] Notably, forensic analysis showed some of these botnets were previously active in Russian criminal organization cybercrime attacks against e-commerce websites.[139]

In the second phase of cyber operations, expert hackers on Russian language web forms recruited novices to participate in cyber attacks that halted or defaced

---

[134] Ibid.
[135] Kagan, Frederick. "It's Not a Cold War." *National Review Online*, August 20, 2008. http://www.aei.org/article/foreign-and-defense-policy/regional/europe/its-not-a-cold-war/ (accessed October 15, 2013).
[136] Ibid.
[137] Bumgarner, John, and Scott Borg. "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008." *US-CCU Special Report* (2009): 6.
[138] Shakarian, Paulo. "The 2008 Russian Cyber Campaign against Georgia." *Military Review-English Edition* 91, no. 6 (2011): 64.
[139] Bumgarner, John, and Scott Borg. "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008." *US-CCU Special Report* (2009): 3.

another 43 websites, including the National Bank of Georgia (which had to disconnect its internet connection for 10 days), CNN and the BBC in Georgia, among many others. The cyber warriors still relied on DDoS, but also manipulated website vulnerabilities using SQL injections[140] to deface President Saakashvili's website, comparing him to Adolf Hitler.

These cyber operations effectively silenced the Georgian media, keeping Georgian nationals in the dark, sowing confusion and sapping morale, while serving to delay an international response.[141] [142]

Cyber attacks such as these require proper surveillance planning, reconnaissance, and coordination in cyberspace, analogous to the preparations for military operations in the physical realm. Subsequent investigations by the U.S. Cyber Consequences Unit (US-CCU),[143] Project Grey Goose, and other cyber security experts revealed that the cyber campaign against Georgia originated from Russian civilian networks aided by Russian organized crime. Additionally, the timing, coordination and sophistication of those attacks indicated a professional level of advanced preparation and reconnaissance.[144] [145] [146]

---

[140] US-CCU called this an "usually sophisticated technique for such a purpose." One researcher describes SQL injection attacks as using "a text field on a webpage to directly communicate with the back end database (normally, a common SQL database – hence the name). A system susceptible to this type of vulnerability essentially gives the hacker total access to the database—including list user login IDs, financial transactions, or website content."

[141] Bumgarner, John, and Scott Borg. "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008." *US-CCU Special Report* (2009).

[142] Ibid.

[143] US-CCU is an independent, non-profit research institute.

[144] Carr, Jeffrey. 2009. *The Evolving State of Cyber Warfare*. Phase 2. Project Grey Goose. http://fserror.com/pdf/GreyGoose2.pdf

[145] Shakarian, Paulo. "The 2008 Russian Cyber Campaign against Georgia." Military Review-English Edition 91, no. 6 (2011).

[146] Bumgarner, John, and Scott Borg. "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008." *US-CCU Special Report* (2009).

According to US-CCU's analysis, at least one of the graphic art images used by hackers to deface a Georgian website was created over two years prior to the 2008 cyber attacks.[147] Further, one of the main websites utilized to recruit would-be cyber warriors, StopGeorgia.ru, went live within hours of the Russian military assault and it included a list of vetted sites to target and toolkits with cyber weapons available for download by novice hackers.[148] [149] The US-CCU investigators explained:

> "Many of the cyber attacks were so close in time to the corresponding military operations that there had to be close cooperation between people in the Russian military and the civilian cyber attackers. When the cyber attacks began, they did not involve any reconnaissance or mapping stage, but jumped directly to the sort of packets that were best suited to jamming the websites under attack. This indicated that the necessary reconnaissance and writing of scripts had to have been done in advance."[150]

The Russian military operations culminated in Georgia losing control of approximately 20 perfect of its territory, as Russia and five other nations recognized South Ossetia and Abkhazia as independent states. [151] An ancillary benefit of this conflict to Moscow was that the value of Russian oil and gas pipelines was bolstered, as investors and oil producers were convinced that the Caucuses are volatile relative to Russian routes from the Caspian Sea.[152] [153] Since the international community

---

[147] Ibid. 5

[148] Krebs, Brian. "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks." *The Washington Post* 16 (2008).

[149] Shakarian, Paulo. "The 2008 Russian Cyber Campaign against Georgia." Military Review-English Edition 91, no. 6 (2011): 64.

[150] Bumgarner, John, and Scott Borg. "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008." *US-CCU Special Report* (2009): 3.

[151] Clarke, Richard A., and Robert Knake. *Cyber War: The next threat to national security and what to do about it*. HarperCollins, 2010: 18.

[152] Bumgarner, John, and Scott Borg. "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008." *US-CCU Special Report* (2009): 7, 8.

offered no real response to the Russian cyber operations and allowed Russia to refuse to identify and arrest the perpetrators, Moscow was able to demonstrate that with a thin veneer of attribution cloaking, it would face no repercussions for offensive cyber attacks.

Insofar as the efficacy of the cyber campaign, one should note that Russia's overwhelming conventional military superiority over Georgia would likely have led to a similar outcome without the cyber component. Cyber weapons caused confusion and decreased morale, frustrated Georgian government officials in their attempts to communicate their plight to the world, and disrupted financial flows. However, these results are typical of traditional military campaigns that attack an adversary's communications systems and command and control structures. The notable difference with the cyber campaign was that attribution was partially obfuscated and cyber warriors' victories were attained without risking the lives of service personnel. Conversely, Tbilisi was able to recover more quickly from the cyber attacks on their networks compared to the damage that would have ensued from a bombing campaign. The limited cyber victory was bloodless (as compared to the other kinetic attacks) but also far less efficacious.

Conclusion

Based on the evidence in each case study, at present it does not appear that the Internet, as an instrument of war or warfare, meets all of Cohen's tests for a transformational military technology. That is not to say that the future possibility of

[153] The American Enterprise Institute, "The War in the Caucasus: An Initial Assessment." Last modified August 13, 2008. Accessed November 7, 2013. http://www.aei.org/files/2008/08/13/20080813_PowerpointPresentation.pdf

cyber weapons being revolutionary is negated based on these two case studies alone; more systematic evaluation is still needed. However, these case studies are not atypical when compared across the spectrum of interstate cyber conflicts accessible for review, and it seems unlikely that other currently available case studies would meet all of Cohen's four criteria for RMA.

With Estonia, some contend that cyber was challenging the rules of the game by allowing Russia to use the anonymity of the Internet via proxies to attack a NATO country thereby negating the nuclear umbrella of protection.[154] However, a state's use of asymmetric methods or proxy groups is not new, even among nuclear-armed states. While the medium of attack (cyber) was new, but the tactics (terrorism) is as old as war itself; ergo the appearance of combat was changed from physical terrorism to cyber terrorism. More importantly, although the fifth domain attacks were greatly frustrating to Estonia, they were temporary in nature and not coercive enough on their own to produce the desired political outcome, a fundamental threshold that must be reached or else acts are reduced to mere criminality.

Figure 1.C – The Cohen Matrix[155]

	Russia vs. Estonia	Russia vs. Georgia
Q1 – Did cyber change the appearance of combat?	**Yes**	**Yes**
Q2 – Did cyber change the structure of armies?	**No**	**No**
Q3 – Did cyber lead to the rise of new military elites?	**No**	**No**
Q4 – Did cyber alter countries' power position?	**No**	**No**

[154] Herzog, Stephen. 2011. Revisiting the Estonian cyber attacks: Digital threats and multinational responses. Journal of Strategic Security 4 (2) (05/01): 51.
[155] Cohen, Eliot A. 1996. A revolution in warfare. Foreign Affairs 75 (03/01): 37.

Russia prosecuted its conflict with Georgia in the physical and cyber domains, and the cyber element proved to be a useful force multiplier in the context of a broader strategic campaign. Yet, in comparing the Russia's conflicts with Estonia and Georgia, it is clear that there is no substitute for physical coercion to compel one's adversary. The cyber component in these contests had some effect, but was not sufficient to alter power positions, structurally change armies or lead to the new military elites.

One cannot rule out the possibility of more severe cyber attacks carrying a greater effect; however, in that case, a state's use of cyber attacks would no longer come with the masking of attribution, which was one of the primary benefits of the cyber tool for Russia. Rather than allowing action with impunity, a state could risk drawing in outside powers and face counterattacks in the physical realm if a cyber weapon with a lethal payload was deployed. Thus, while cyber enables a state to hide its hand, the covert nature necessitates that its results be relatively constrained.

One could envision a hypothetical future where the pace of technology progresses in such a manner that traditional comprehensions of warfare are overturned. What were considered at the time to be groundbreaking cyber attacks against Estonia and Georgia, five years later are considered a "bad joke" by technical experts: if executed today against websites like Amazon or Google, they would do so little damage that they may not even be noticed.[156]

[156] McGraw, Gary, and Nathaniel Fick. *Separating Threat from the Hype: What Washington Needs to Know about Cyber Security*. *America's Cyber Future, Volume II*. CNAS, 2011.

Certainly, militaries will continue to develop their doctrines for using the Internet as a tool of state power and in preparing their defenses against foreign cyber attacks. However, the way that these developments will proceed is as yet unknown. In the absence of a generally accepted framework for the military's use of the Internet, it would be prudent for policymakers to at the very least agree on a definition of cyber war and establish international norms for cyber conflict to increase predictability and avoid unintended military escalation. Such norms might designate civil cyber infrastructure as out of bounds in interstate conflict, and focus on defense of the civilian networks to hedge against unforeseeable threats. As Cohen theorized 17 years ago, the world may be on the edge of an information-led transformation of war, but it is not yet at the point where one can declare that the revolution is upon us.

CHAPTER 2 - THE ROLE OF INTERNET AND COMMUNICATIONS TECHNOLOGIES IN MODERN IRANIAN REVOLUTIONARY MOVEMENTS

Harvard Law professor Yochai Benkler posits that the global economy is undergoing a structural change caused by ICT, which is producing an emerging "networked information economy," and resulting in more freedom for democratic societies.[157] The second chapter of this thesis uses Iran as case study to evaluate the phenomenon of ICT and its effects on internal state security. This chapter will test the notional argument that ICT creates a "competitive advantage" for dissidents inside authoritarian states, thus making revolution a more likely outcome.[158] This chapter will also review and evaluate the theoretical approaches of Internet utopians and their critics. To understand the applicability of ICT in Iran, this chapter will examine the historical relevance of media and communications tools in Iran during prior reform and revolutionary movements. Finally, this chapter will analyze present uses of ICT in Iran by both agency and the state, to determine whether ICT is working to the advantage of the Green Movement or the current regime.

Literature Review

Theoretical approaches can inform our understanding of the Internet phenomenon by providing an intellectual framework in which these questions can be addressed: Is there a causal relationship between ICT and successful revolutionary movements? If individuals have more access to ICT in authoritarian states, is the likelihood of revolution increased? Conversely, are ICT and

[157] Benkler, Yochai. *The Wealth of Networks* (New Haven: Yale University Press, 2006), 1-3
[158] Shirky, Clay. "The Net Advantage," *Prospect*, December 11, 2009, http://www.prospectmagazine.co.uk/2009/12/the-net-advantage/ (accessed September 12, 2010).

revolutionary movements simply correlated experiences due to a more globalized world?

The incipient schools of thought regarding the Internet, its defining characteristics, inherent values, and potential transformative capabilities can be delineated into three generalized categories: The first group are "techno-optimists" or Internet utopians,[159] the second group are ICT pragmatists, and the third is a group consisting of ICT pessimists. The principal point of contention between these groups is the value they ascribe to the Internet. Internet utopians contend that ICT is innately democratic, while pragmatists and pessimists in general see these tools fundamentally as value neutral. However, both utopians and pragmatists agree the Internet is shifting power differentials in favor of the individual, but pessimists view this as a slow evolution and a dramatic shift to the individual is futuristic, and maybe not even likely at all. Pessimists argue the nation state remains the most powerful actor as it still has a monopoly on the use of force; as such, the nation state maintains the power advantage, particularly in autocratic states. All other arguments and tangential discussions extend from this primary judgment.

Prior to a lengthy theoretical review, some basic concepts about the Internet must be explained. First, the Internet is a transnational telecommunications system connected by a series of networked computers connected to other networked computers around the world, otherwise known as a "network of networks."[160] [161] This Internet system has profound economic and social implications. Economists

[159] Bremmer, Ian. "Democracy in Cyberspace." *Foreign Affairs* 89 no. 6 (2010): 87.
[160] "A Virtual Counter-Revolution," *The Economist*, September 4, 2010, 75.
[161] "Internet Basics," Florida Center for Instructional Technology, http://fcit.usf.edu/Internet/chap1/chap1.htm. (accessed November 19, 2010).

view the Internet as having "network effects" meaning that since the costs for entry are very low, individuals are more likely to join and create.[162] [163] Second, it is a "generative" and open platform unlike any other mass media in history in that users are both consumers and producers of information.[164] Third, the unprecedented speed at which information is transferred across national borders has limited distance and time making the Internet an efficient distribution center with the ability to serves as a megaphone for ideas or products.[165] Conversely, the Internet's stated attributes can also make information overly diffuse and saturated to the point of overload.

Internet Utopians, Pragmatist and Pessimists

As stated previously, Internet utopians ascribe democratic values to ICT but their belief in the technology's scope is far more ubiquitous. For early utopians, the Internet was a revolutionary tool ushering in a new information age in which the limitations of time, space and distance were being erased.[166] [167] One of the first techno-optimists, John-Perry Barlow, went so far as to claim the Internet would end the nation state as we know it, purporting the disappearance of borders due to the Internet because states could no longer declare sovereignty on the web.[168] By purporting this sublime view of ICT Barlow ignored the very real physical domain of the Internet in which servers, computer platforms, cable modems, and electrical

[162] "A Virtual Counter-Revolution," *The Economist*, September 4, 2010, 75.
[163] Nye, Joseph. "Cyber Power", http://web.mit.edu/ecir/pdf/nye-cyberpower.pdf (accessed October 16 2010).
[164] "A Virtual Counter-Revolution," *The Economist*, September 4, 2010, 76.
[165] Bremmer, Ian. "Democracy in Cyberspace." *Foreign Affairs* 89 no. 6 (2010): 88.
[166] "A Virtual Counter-Revolution," *The Economist*, September 4, 2010, 75.
[167] Bremmer, Ian. "Democracy in Cyberspace." *Foreign Affairs* 89 no. 6 (2010): 86.
[168] "A Virtual Counter-Revolution," *The Economist*, September 4, 2010, 75.

power all exist inside the borders of nation-states.[169] While Barlow saw ICT as enabling the end of the sovereign state, Anne-Marie Slaughter argues the result of ICT is realignment in global powers leading to the "relative decline of U.S. influence".[170] Slaughter posits that in the twenty-first century, state power is measured by "connectedness" because the new "networked world… exists above the state, below the state and through the state."[171] However, she continues this line of thinking by suggesting the U.S. can avoid decline by harnessing the power of networked ICT to sustain its competitive edge.[172]

For many of these scholars and other Internet utopians, the pervasive spread of information by interconnected ICT is as transformative as the division of labor preached by Adam Smith prior to the Industrial Revolution. But scholars are not the only proponents of a globalized or networked new world order created by ICT: neoconservatives, classical liberal economists, business persons, Marxists, politicians, journalists and even the current Secretary of State, Hillary Clinton, with her "21st Century Statecraft" program find ICT to be global homogenizing force for good.[173] Secretary Clinton's overvaluation of ICT led her to call on the Twitter's corporate headquarters to delay routine maintenance to allow protestors in Iran to continue using the Twitter website. As the United States took no firm steps to

[169] Nye, Joseph. "Cyber Power", http://web.mit.edu/ecir/pdf/nye-cyberpower.pdf (accessed October 16 2010).
[170] Slaughter, Anne-Marie. "America's Edge," *Foreign Affairs*, (January/February 2009), http://www.foreignaffairs.com/articles/63722/anne-marie-slaughter/americas-edge (accessed December 8, 2010).
[171] Ibid. 1
[172] Ibid. 1,2
[173] "21st Century Statecraft," U.S. Department of State, http://www.state.gov/statecraft/index.htm (accessed November 19, 2010).

support the Green Revolution, it appears in this case Washington saw technology as a strategy unto itself rather than as a tool for tactical advantage.

More nuanced theories have developed since the early days of the Internet. While many scholars espouse ICT's attributes (speed, time, distance, diffusion, efficiency and social connectivity) are fundamentally changing existing structures, the merits and degree of those changes are not agreed upon. Leading scholars, such as Internet utopians like Yochai Benkler, Clay Shirky, and David Weinberger, have all examined the new networked world and purport that the Internet is instinctively good due to its supposed democratic characteristics and is therefore a unifying and progressive trend for society. For the utopians, since the Internet functions as a network of networks, the emphasis must be on the collective, making it intrinsically democratic. This new asymmetry of the empowered individual, it is argued, affords a never-before available competitive advantage to dissidents living in authoritarian states. ICT pragmatists and pessimists will of course take issue with this theory. Ian Bremmer writing in Foreign Affairs explains, "…if greater openness creates new opportunities, it also creates new worries."[174]

ICT pragmatists like Joseph Nye and Ian Bremmer agree that interconnected information age has seen a "diffusion of power to the non-state actor" [the individual], but argue ICT is not necessarily democratic since it empowers anyone who willing to use it including criminals and terrorists.[175] In Nye's assessment of ICT entitled "Cyber Power", he recognizes the "great complications" all nation-states

[174] Bremmer, Ian. "Democracy in Cyberspace." *Foreign Affairs* 89 no. 6 (2010): 91.
[175] Nye, Joseph. "Cyber Power", http://web.mit.edu/ecir/pdf/nye-cyberpower.pdf (accessed October 16 2010).

face in light of this new information age.[176] According to Nye, the individual is increasingly at advantage in the cyber domain due to three factors: "low cost if investment for entry, virtual anonymity and ease of exit."[177] Governments are increasingly vulnerable in the cyber realm because the benefits afforded to individuals by ICT. It is the nature if the Internet that makes power differentials between the state and the individual reduced, he explains.[178] Nye's discourse on cyber power dynamics and asymmetry is foundational for understanding other Internet utopian concepts, such as Net advantage, but his optimism is hedged by his underlying assumption that nation states will still remain the strongest actors for some time, making him a pragmatists.[179]

Where Internet utopians, and to a lesser degree ICT pragmatists, envisage a new world order enabled by the Internet that is more democratic and more free, ICT pessimists see communications tools that give the illusion of power to a minority of activists while authoritarian states use the Internet as an "new opium for the masses."[180] The utopians have placed far too much emphasis on individuals while ignoring the inevitable response to power differentials by the nation state. For example, Rebecca MacKinnon has observed the evolution of the Chinese attitudes

[176] Ibid.
[177] Ibid.
[178] Ibid.
[179] Ibid.
[180] Morozov, Evgeny. "How dictators watch us on the web," *Prospect*, (November 18, 2009) http://www.prospectmagazine.co.uk/2009/11/how-dictators-watch-us-on-the-web/ (accessed September 18, 2010).

towards technology described in a new term she coined "networked authoritarianism."[181]

The Chinese and the Iranian authorities do not employ wholesale Internet prohibition (except in extreme, time-limited cases) because their economies are equally dependent on communications technology, but rather they have evolved to a new generation of "censorship techniques" that "shape the users' online experience in ways that are largely unseen."[182] This networked authoritarianism allows the governments of China and Iran to gain the economic benefits of globalized ICT without the activism that could possibly challenge their regimes.[183] The information revolution could still lead to entropy as autocrats still desire control of their populations; the Internet has not changed the dictator's strategic interest in maintaining his regime and he will not go quietly.

Pessimists like Malcolm Gladwell, Eygeny Morozov, Rafal Rohozinski and Ronald Deibert also contend ICT cannot deliver on the revolutionary promises its enthusiasts purport because the Internet is not a substitute for "high-risk activism" which leads to tangible social or political change.[184] Gladwell further advances this theory by arguing the Internet and social media may connect more diverse groups of people than before, but these ties are weak and they result in more participation in

[181] Currie, Kelley. "The Battle over Internet Freedom," The Weekly Standard, (October 26, 2010) http://www.weeklystandard.com/blogs/battle-over-internet-freedom_512987.html (accessed October 31, 2010).
[182] Ibid.
[183] Ibid.
[184] Gladwell, Malcolm. "Small Change," *The New Yorker*, (October 4, 2010) http://www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell (accessed October 11, 2010), 4.

activities that do not require a significant amount of personal sacrifice.[185] Most critically Gladwell writes, "The instruments of social media are well suited to making the existing social order more efficient. They are not the natural enemy of the status quo."[186]

Deibert and Rohozinski also discourage the illusion that there can ever be a technological silver bullet capable of ushering in democracy. They write "Liberation, freedom, and democracy are all socially contested concepts and thus must be secured by social and political means."[187] A communications tool cannot produce a democracy; that is a political choice that must be made by humans. The larger question then becomes: If the appropriate amount of high-risk activists are in place, can ICT act as a catalyst to aid in opening up authoritarian states as it has opened up countries to commerce globally?

Internet theory is naturally an incipient field of study where the leading schools of thought are still forming conceptual models for expression. However, there are three theories by Internet utopians that require further exploration to have a full view of the topic. These three ideas are highlighted below.

The Net Advantage

Clay Shirky, a leading authority on ICT's social implications and techno-optimists, created the concept of "Net Advantage" which he spelled out in his best seller, *Here Comes Everybody: the Power of Organization without Organizations*, and subsequent writings. Simply put, Shirky purports the Internet has reshaped social

[185] Ibid. 3-6
[186] Ibid. 6
[187] Deibert, Ronald and Rafal Rohozinski, "Liberation VS. Control: The Future of Cyberspace," *Journal of Democracy* 21, (2010): 55.

communications and civic life through social media, creating "political information cascades" which encourage more people to resist the regime and bestowing competitive advantage to the dissident.[188]

Shirky's new take on information cascades begins with political scientist Susan Lohmann's theory that when a localized group is willing to publically protest a regime and the authority's reaction is muted, it visibly encourages the "fence-sitters" to join in the next round of protests.[189] Further, if the regime overreacts, it risks delegitimizing itself.[190] Shirky argues ICT presents a new dynamic in dissident protests whereby the information cascade is visible to more people at a faster pace than ever historically possible and additionally, to a wide international audience. Also, ICT offers dissidents the ability to coordinate action despite living under an authoritarian regime, thus persuading more fence sitters to join their cause.

New Public Spheres

John Kelly and Bruce Etling underscore a noteworthy point about the Internet and social change: there is a vital need for public spheres for debating and exchanging ideas. They point to John Dewey who spoke about the necessary "conjoint communicated experience", which is a requirement for democracy.[191] Yochai Benkler expounds on the Dewey idea of a necessary public space by arguing that compared to the older mass media models, ICT is democratic and inclusive, and will always undermine the powerful, even if the take action against those using the

[188] Shirky, Clay. "The Net Advantage," *Prospect*, December 11, 2009, http://www.prospectmagazine.co.uk/2009/12/the-net-advantage/ (accessed September 12, 2010).
[189] Ibid.
[190] Ibid.
[191] Kelly, John and Bruce Etling, "Mapping Iran's Online Public." *Berkman Center Research Publication* no. 2008-01 (2008): 22.

Internet as a weapon against their regime.[192] Benkler argues the Internet is a public space that will always give competitive advantage to the individual.

New Ecology of Activism

David Weinberger, a senior researcher at Harvard's Berkman Center, has proposed a theory that the Internet is changing the ecology of human social behavior. While he is dubious of the prognostication that the Internet will ineluctably cause regime change, Weinberger does argue ICT is affecting traditional institutions by changing how they work.[193] When anyone with interest via the Internet can participate, it changes the characteristics of how that organization operates. To justify this assertion, Weinberger uses the example of journalism and citizen journalists operating in the blogosphere: Professional journalists still exist but the dynamics of the news business have been transformed by individual bloggers who can challenge the status quo.

Case Studies

Since the introduction of the telegraph in the 1850s, communications tools in Iran have been applied by both State power structures and agents of opposition for their own purposes: autocratic Shahs like Nasser-iddin and Mohammad Reza Pahlavi have used communications tools as a powerful but limited weapon of propaganda to defend the legitimacy of their regimes or to expand their writ.[194] Conversely, opposition leaders like Sayyed Jamal ad-Din and Ayatollah Ruhollah

---

[192] Ibid. 23

[193] Weinberger, David. "Gladwell discovers it takes more than 140 characters to overturn a government," (accessed October 2, 2010) http://www.hyperorg.com/blogger/2010/10/02/gladwell-discovers-it-takes-more-than-140-characters-to-overturn-a-government/ (accessed October 16, 2010).

[194] Keddie, Nikki. *Modern Iran: Roots and Results of Revolution* (2 ed. New Haven: Yale University Press, 2006), 54.

Khomeini have usurped the intended purposes of the State's communications tools to spread their own revolutionary ideologies by creating a space for debate and public mobilization.[195] [196]

Tobacco Protests and Constitutional Revolution

The introduction of modern communications tools in Iran, like the telegraph and radio, were exogenous events. Nasser-iddin Shah in the 1850s sought from the British government a rudimentary telegraph network to connect Tehran with its outlying provinces and thereby allow Nasser-iddin to exert greater control over some of Iran's volatile ethnic groups.[197] The British eagerly sponsored the creation of an extensive national telegraph network later in the 1860s and 1870s because they sought more control over colonized India through Iran.[198] Iran scholar Ervand Abrahamian notes, "The telegraph network, expanding to cover nine thousand miles by 1900, connected not only London with India, but also Tehran with the provinces, and thus the Shah with his provincial administrators."[199] The more expansive British telegraph network, although initially resisted by the Shah, provided Iran a modern way to communicate with the outside world and was an important source of revenue for the monarchy.[200] While envisaged as a medium to further consolidate monarchial rule by both the Iranian and British crowns, the telegraph was then seized upon by the opposition to subvert the monarchies, specifically

[195] Ibid. 54
[196] Sreberny-Mohammadi, Annabelle and Ali Mohammadi. *Small Media, Big Revolution* (Minneapolis: University of Minnesota Press, 1994), 31.
[197] Sreberny-Mohammadi, Annabelle and Ali Mohammadi, *Small Media, Big Revolution* (Minneapolis: University of Minnesota Press, 1994), 44.
[198] Abrahamian, Ervand. *Iran between Two Revolutions* (Princeton: Princeton University Press, 1982), 57.
[199] Ibid. 57
[200] Sreberny-Mohammadi, Annabelle and Ali Mohammadi, *Small Media, Big Revolution* (Minneapolis: University of Minnesota Press, 1994), 45.

during the tobacco protests of the early 1890s and the constitutional revolution of 1906.[201]

As the first early form of modern media, the telegraph served to import ideas, cultures, news and experiences from the outside world into Iran. It helped establish the first newspapers in Iran by capturing wire stories from Reuters that were intended for use by the Indian press.[202] At times the Shah's opposition leveraged the telegraph by sending messages to Paris and London asking for assistance from Western nations against the regime, much to the Shah's chagrin.[203]

The Shah's tobacco concession to the British monopoly in 1890 ignited the agrarian, clerical, and bazaar classes in revolt. The telegraph, in combination with the stinging criticism in leaflets by the Islamist Sayyed Jamal ad-Din "al-Afghani", helped speedily enrage Iranian citizens who otherwise would have heard of the outbreak of protests among their fellow citizens much later.[204] The telegraph's quick dissemination of information helped fuel widespread discontent and general strikes, and in combination with a *fatwa* ignited protests in six cities: Tehran, Isfahan, Tabriz, Mashad, Qazvin, Yazd and Kermanshah.[205] More importantly, these protests allegedly revealed that realignment was underway in Iranian society enabled by modern communications. As Abrahamian explains, "The crisis revealed the fundamental changes that had taken place in nineteenth-century Iran. It

[201] Keddie, Nikki *Modern Iran: Roots and Results of Revolution* (2 ed. New Haven: Yale University Press, 2006), 60-63.
[202] Sreberny-Mohammadi, Annabelle and Ali Mohammadi, *Small Media, Big Revolution* (Minneapolis: University of Minnesota Press, 1994), 45.
[203] Ibid. 46
[204] Keddie, Nikki. *Modern Iran: Roots and Results of Revolution* (2 ed. New Haven: Yale University Press, 2006), 61.
[205] Abrahamian, Ervand. *Iran between Two Revolutions* (Princeton: Princeton University Press, 1982), 71.

demonstrated that local revolts could now spread into general rebellions; that the intelligentsia and the traditional middle class could work together."[206]

After a major demonstration in Tehran where security forces killed many unarmed protestors, the Shah was forced to recant his concessions to the British. The experience afforded the opposition with its first successful reform by way of mass protests from a united cross section of Iranians: the clergy, intelligentsia, "bazaaris", and average citizens.[207] Iranians had now tasted the fruits of free expression and yearned for more, in particular, a constitution and the rights it afforded citizens.[208] However, the uprising among Iranian citizens, first against perceived repressive economic policies and then later in the 1906 constitutional crisis, would not prove ultimately successful on a grand scale again for another 88 years.

By extrapolating from the early experiences with the telegraph, three conclusions can be reached: that communications tools uniquely enabled the spread of ideologies and information beyond the control of the State; that regime's intended purpose for the telegraph could be subverted by opposition groups for political mobilization; and that because of the speed and distance of the telegraph's reach, elites in other countries could be alerted of dissidents' grievances inside a closed regime in remarkable speed.

---

[206] Ibid. 73
[207] Keddie, Nikki. *Modern Iran: Roots and Results of Revolution* (2 ed. New Haven: Yale University Press, 2006), 62.
[208] Ibid. 72

Stated Dominated Communications

The telegraph's early use foreshadowed how future media would empower Iranians to utilize technological innovation for dissident purposes. Radio was introduced to Iran when the German army established a connection using long-wave radio with Isfahan in 1915.[209] In 1924 Mohammad Reza Shah Pahlavi's father, Reza Shah Pahlavi, arranged with the Soviets to obtain the first wireless telegraph, which would beget a radio broadcasting system by 1935.[210] This technological advancement initially made the military more efficient. The desire for radio broadcasting began with the military but it was further expanded because Reza Shah and his security apparatus believed in the inherent propaganda value of radio.[211] Reza Shah's sympathetic views towards the German Nazis during the Second World War eventually landed him on the wrong side of the Allies, who forced him to abdicate the throne in 1941.[212] Just prior to the Shah's departure, the British Broadcasting Corporation (BBC) in 1940 began a Persian language service to exert more influence over an Iran that many in the West feared was too cozy with the Germans.[213]

Mohammad Reza Shah's vision for a developed, modern state-planned society included support for the creation of broadcast media.[214] The Shah sought to project his desired image of Iran into the homes of his citizens via the popular

[209] Ibid. 52
[210] Ibid
[211] Ibid. 53
[212] Keddie, Nikki. *Modern Iran: Roots and Results of Revolution* (2 ed. New Haven: Yale University Press, 2006), 105.
[213] Herrmann, Steve. "Social Media in Iran," *BBC*, June 16, 2009, Tuesday; online edition, http://www.bbc.co.uk/blogs/theeditors/2009/06/social_media_in_iran.html (accessed November 1, 2010).
[214] Tehranian, Majid. *International Journal of Middle East Studies* (1995), http://www.jstor.org/pss/176378 (accessed July 17, 2010), 226.

mediums of radio and television. The Shah's top-down approach to media sought to "manufacture legitimacy" for his rule, as was consistent with contemporary theories of modernization since he viewed media as a utilitarian means to spread modern social norms.[215] Concurrently, rigid censorship of independent journalists and a muted political climate greatly limited the development of Iranian civil society and offered no forum for political debate, all to accomplish the Shah's vision of a nationalist and almost anti-clerical modern Iranian state.[216] In short, "Big media became the tool of [a] big authoritarian [state]."[217]

Unlike the telegraph and radio, television's introduction into Iran resulted from the domestic private sector and American innovation, rather than from a state-centric dictatorial plan. The pioneering and well-connected Sabet family received approval from the Shah and through the *Majilis* to build a television broadcast system in Tehran. In 1958, the Sabet's first broadcast went live with an orchestrated speech from the Shah.[218] However, a medium so powerful and compelling like television would not last long outside state control: by 1966, the Plan and Budget Organization began allocating funds for television development and procurement. In October of that year, the state-owned National Iranian Television was born and eventually overtook the Sabet family's organization.[219] For the Shah, television was instrumental in solidifying his attempts to remake Iran into

[215] Ibid. 226
[216] Sreberny-Mohammadi, Annabelle and Ali Mohammadi, *Small Media, Big Revolution* (Minneapolis: University of Minnesota Press, 1994), 88- 89.
[217] Ibid. 5
[218] Sreberny-Mohammadi, Annabelle and Ali Mohammadi, *Small Media, Big Revolution* (Minneapolis: University of Minnesota Press, 1994), 62.
[219] Ibid. 66

his nationalist vision; by 1974, televisions were in the homes of an estimated 15 million, or about half of the population.[220]

Media Makes Revolution?

The causality of the Iranian revolution is an often-debated subject since the overthrow of the Shah in 1979. While this paper will not address causality of the 1979 revolution, a subject more appropriately covered in book volumes, it is important to review the role media played. Theda Skocpol, a foremost scholar on the French, Russian and Chinese Revolutions, notes the Iranian experience was quite unique from the "classical" revolutions of the past. The 1979 Iranian revolution was both a social and political revolution fueled by rapid modernization, which Skocpol had argued in her early works was not possible.[221] The Iranian revolution also was not characteristic of other historical revolutions that were led by the lower classes, as Skocpol had again contended in earlier works.[222]

In stark contrast, the Iranian revolution was an amalgamation of social classes with the educated urbanites and religious elites leading the way. Additionally, Skocpol admits to being vehemently critical of those who suggested revolutions were orchestrated or could ever be "made."[223] To her credit, Skocpol writing in 1982 suggests the Iranian revolution, "…did not just come; it was deliberately and coherently made."[224] The purpose of addressing the revolutionary causality is to understand what role the media may have played in the orchestration

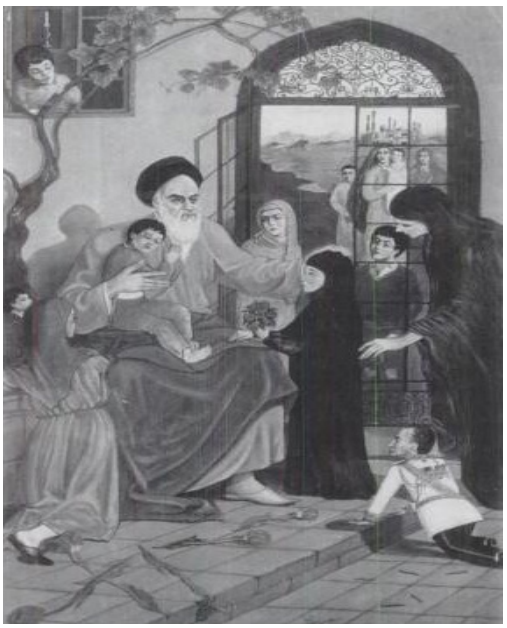
[220] Fathi, Asghar. "The Role of the Islamic Pulpit." *Journal of Communications* 29, no. 3 (Sumer 1979): 102-105.
[221] Skocpol, Theda. "Rentier State and Shi'a Islam in the Iranian Revolution," *JSTOR*, 265-267, http://www.strongwindpress.com/pdfs/TuiJian/SkocpolRentierStateIran.pdf (accessed July 14, 2010).
[222] Ibid. 266
[223] Ibid. 266
[224] Ibid. 267

of the revolution. The social discontent was guided and fueled in part by Ayatollah Khomeini's mass-propaganda via the cassette tapes or "electronic pulpit" (*minbar*) and photocopied posters, night letters and political statements (*elamieh*).[225] With regard to the use of media to foment discontent, Khomeini himself said, "Propaganda is [as] explosive as a grenade."[226]

Differing somewhat from the opposition during the tobacco protests and the Constitutional crisis, Khomeini and other dissidents did not initially co-opt mass media; instead he and his followers subverted the Shah's state-controlled "big media" conventions (I.e. Television and radio) with creative "small media" tactics. Small media tools, such as the cassette tape and photocopier, performed the vital functions revolutionary movements need under authoritarian regimes: propagating the masses with radical ideology and serving as a tool for mobilization.

[225] Sreberny-Mohammadi, Annabelle and Ali Mohammadi, *Small Media, Big Revolution* (Minneapolis: University of Minnesota Press, 1994), 118 & 119.
[226] Peterson, Scott. "Khameini's visit to Qom shows the power of propaganda," *Christian Science Monitor*, October 28, 2010, http://www.csmonitor.com/World/Global-News/2010/1028/Khamenei-s-visit-to-Qom-shows-the-power-of-propaganda (accessed December 4, 2010).

Figure 2.A - Ayatollah Khomeini and the Shah[227]



Annabelle Sreberny-Mohammadi and Ali Mohammadi writing in *Small Media, Big Revolution* testify about their firsthand accounts of small media as a "catalyst for political participation" in the Iranian revolution.[228] Long before "twitter revolutions" were in vogue, the Mohammadis advanced a communications theory of revolution to be applied specifically to authoritarian states: "mediated culture has become part of the causal sequence of revolutionary crisis, as well as central to revolutionary process."[229] However, they are very cautious to avoid determinisms; small media by itself does not make revolution.[230]

[227] Sreberny-Mohammadi, Annabelle and Ali Mohammadi, *Small Media, Big Revolution*, 93: "Here Khomeini appears in a Christ-like pose, 'suffer the little children to come unto me' as they do from far and wide on a pilgrimage, signifying the true imami status of Khomeini. The vine signifies paradise where the fallen martyrs (the tulips) will go, as Khomeini blesses their offspring. A pathetic little Shah clambers on his knees over spent bullets – himself asking for blessing/forgiveness?"
[228] Ibid. 31
[229] Ibid. 19
[230] Ibid. 37

Khomeini's propaganda successes during the revolution were in large part due to five factors: he was a charismatic authority figure who became the de facto leader of the popular revolt[231]; a broad based coalition supported the movement (largely due to clerical organization)[232]; they had a clear message "Death to the Shah"[233]; a clear political goal "independence, freedom, Islamic Government"[234]; and the military was incapable or unwilling to act against them.[235] Khomeini's genius was not just his inventive use of media but rather the application; he harnessed traditional social and religious networks to spread revolutionary sentiments rapidly through audiocassettes and photocopied leaflets.[236]

Since independent political parties and a free press were not permitted under the Shah, the alternative public sphere became the deeply socially integrated mosque network. In essence, small media in Iran can be thought of as the first forms of what is defined today as "social media". For example, the modern podcast or YouTube clip is analogous to Khomeini's cassette tapes. These illicit communications distributed through influential social and religious channels allowed for the underground dissident movement to gain strength despite the watchful eyes of the SAVAK[237]. The Shah notably underestimated the compelling nature of Khomeini's taped sermons by allowing his relocation to Paris. Being in

[231] Ibid. 118
[232] Ibid. 119
[233] Ibid. 118
[234] Ibid.
[235] Skocpol, Theda. "Rentier State and Shi'a Islam in the Iranian Revolution," *JSTOR*, 267, http://www.strongwindpress.com/pdfs/TuiJian/SkocpolRentierStateIran.pdf (accessed July 14, 2010).
[236] Sreberny-Mohammadi, Annabelle and Ali Mohammadi, *Small Media, Big Revolution* (Minneapolis: University of Minnesota Press, 1994), 119-125.
[237] Translates to the "Organization of Intelligence and National Security".

Paris enabled the reproduction and worldwide distribution of Khomeini's cassette-taped sermons and raised his profile on the international stage.[238]

The Iranian example of "small media" networks successfully fomenting ideological dissent inside closed states and more importantly, in organizing an opposition movement, should be balanced with knowledge of the international notoriety that Khomeini gained in Paris. In his first eight weeks in France, Khomeini took full advantage of the international press, sitting for interviews with *Le Monde*, the Associated Press, French, German, Austrian, Swedish and Greek broadcasters, America's CBS News and Britain's *The Guardian* newspaper.[239] For someone with virulent anti-Western and anti-American sentiments, Khomeini shrewdly managed a public relations campaign that validated his messianic image both at home and abroad.

There is historical precedence in Iran, from the tobacco protests and the 1979 revolution to the Green Movement today, where opposition groups have either usurped the state's control over mass media for revolt; or utilized small media distributed through traditional social networks to undermine the authoritarian regimes. With each historical example observed, it becomes apparent that communications tools have provided dissidents with the ability to mobilize, as well as offer an open space to disseminate revolutionary ideals; however, theorists and historians still debate whether communications tools are proximate to change or ultimate causes of change. If media were an ultimate cause of change, then its

[238] Keddie, Nikki. *Modern Iran: Roots and Results of Revolution* (2 ed. New Haven: Yale University Press, 2006), 233.
[239] Ibid. 134

performance record has thus been unreliable and produces only a marginal success rate when viewed in context.

Iran's Twitter Revolution?

The final section of this paper will analyze the so-called Green Movement in Iran as a case study to test the thesis questions posed at the start. In authoritarian states, does the Internet provide dissidents with a comparative advantage to force desired social or political changes? The Iranian conundrum presents the most relevant case study available as the conflict between the nation state and the individual, empowered by ICT, promulgated the popular notion that a "twitter revolution" could result in regime change.

To outside observers, the Green Movement in Iran appeared to be an anomaly: a sudden awakening of Iranians who were propelled forward in protest against the Presidential election results due to the innovative uses of the Internet and social media tools.[240] Regime critics in the West, most prominently *The Atlantic* blogger Andrew Sullivan, declared "the sound of the next revolution" was underway.[241] That specious interpretation of the election protesters has become conventional wisdom but ignores Iran's long legacy of civil disobedience. Iranian professor and author, Azar Nafisi, explains, "…there is always something going on in Iran…a girl like Neda, had been part of Iranian society as long as I can remember."[242]

---

[240] Peterson, Britt. "A Forgotten Civil Society," *Foreign Policy* (June 7, 2010) http://www.foreignpolicy.com/articles/2010/06/07/a_forgotten_civil_society (accessed June 25, 2010).
[241] Sullivan, Andrew. "The Revolution Will Be Twittered," *The Atlantic*, (June 13, 2009) http://andrewsullivan.theatlantic.com/the_daily_dish/2009/06/the-revolution-will-be-twittered-1.html (accessed December 30, 2010).
[242] Peterson, Britt. "A Forgotten Civil Society," *Foreign Policy* (June 7, 2010) http://www.foreignpolicy.com/articles/2010/06/07/a_forgotten_civil_society (accessed June 25, 2010).

This chapter has documented the ample historical evidence of media used by individuals against the state in Iran: from the telegraph during the Tobacco and Constitutional revolution over 100 years ago, to the use of "small media" in the 1979 Islamic Revolution, journalists and student communiqués in the Khatami years, and social media (like Twitter and Facebook) in the 2009 Presidential election protests.[243] The events of 2009 should be judged in the historical context of Iran's press and media legacy. The precedent can offer some hope for budding reformists; but revolutionaries and their Western supporters should proceed with caution in assuming the Internet is a panacea for all of the problems that ail Iran and other troubled states.

The Green Movement

The Green Movement began as a mass rejection of the alleged fraudulent June 12, 2009 Presidential election results; however, some academics argue the roots go back much further to the Persian quest for democracy during the Iranian Constitutional Revolution of 1906.[244] Former Presidential interpreter, Hooman Majd, sees the Green Movement as an expansive outgrowth of the *mowj-e-sabz* or "the green wave", which was the tech-savvy political campaign to support Presidential candidate Mir Hossein Mousavi.[245]

[243] Eslahchi, Morteza. "Tavaana Interview Transcript," Tavaana, http://www.tavaana.org/nu_upload/Morteza_Eslahchi_En.pdf (accessed December 12, 2010).
[244] Milani, Abbas. "The Green Movement," United States Institute of Peace, http://iranprimer.usip.org/resource/green-movement (accessed December 5, 2010).
[245] Majd, Hooman. "Think Again: Iran's Green Movement," *Foreign Policy*, (January 6, 2010) http://www.foreignpolicy.com/articles/2010/01/06/think_again_irans_green_movement (accessed January 6, 2010).

The Green Movement's name derives from a green sash given to Mousavi by the former reformist President, Mohammad Khatami.[246] It is understood that Mousavi chose green because the color is also associated with the descendants of the Prophet Mohammad (Mousavi is counted as one).[247] Ostensibly, the Green Movement leaders[248] were Mousavi and his wife Zahra Rahnavard but other notable figures include the movement's spiritual leader, Ayatollah Ali Montazeri (deceased December 2009), and reforms advocate Mehdi Karroubi (also a 2009 Presidential candidate).[249] In opposition were the Supreme Leader Ayatollah Ali Khameini, President Mahmoud Ahmadinejad, and former President Akbar Rafsanjani (originally a supporter of the Greens and then sided with Khameini).[250]

In 2009, the structure and nature of the Green Movement was amorphous. The movement began as a rejection of the election that kept Ahmadinejad as President, when three million protestors poured onto the streets of Tehran in opposition to what appeared to be fabricated ballot results.[251] The early phases of the Green Movement were not an organized hierarchy; rather, it was akin to a non-violent mob where the participants chanted, "Where is my vote?"[252] Mousavi's green wave "morphed" from an election campaign into a mass protest

[246] Ibid.
[247] Cole, Juan. "The Greens in Iran are a Movement, not a Coup," Informed Comment, (June 13, 2010) http://www.juancole.com/2010/06/the-greens-are-a-movement-not-a-coup.html (accessed December 17, 2010).
[248] Note: Some factions of the Green Movement claim to be leaderless.
[249] Milani, Abbas. "The Green Movement," United States Institute of Peace, http://iranprimer.usip.org/resource/green-movement (accessed December 5, 2010).
[250] Ibid.
[251] Ibid.
[252] Ibid.

demonstration and then to a social movement and civil rights movement, producing the largest and broadest reform coalition since the 1979 revolution.[253] [254]

Equally, the movement's goals appeared to evolve throughout 2009 and 2010. Mousavi campaigned on a platform of reform within the existing paradigm, which is a theocratic authority (*vilayat-e faqih*) that supervises the semi-democratic elected officials including the president and members of the parliament (*Majilis*). It is vital to understand that Mousavi's green wave election campaign spoke of reform rather than revolution and that Mousavi praised the Supreme Leader during his campaign speeches.[255]

In general, the early Mousavi supporters and the green movement protestors were not iconoclasts. They did not demand an overthrow of the Islamic government either. Rather, they called for an investigation of the fraudulent election and with the possibility of a new election to ensure their votes would be properly counted.[256] It was not until the brutal crackdowns by Iran's security forces and the systemic rape and torture of dissidents in Evin prison that protesters directly attacked the

[253] Cole, Juan. "The Greens in Iran are a Movement, not a Coup," Informed Comment, (June 13, 2010) http://www.juancole.com/2010/06/the-greens-are-a-movement-not-a-coup.html (accessed December 17, 2010).
[254] Majd, Hooman. "Think Again: Iran's Green Movement," *Foreign Policy*, (January 6, 2010) http://www.foreignpolicy.com/articles/2010/01/06/think_again_irans_green_movement (accessed January 6, 2010).
[255] "Mousavi praises Leader's New Year message," *Tehran Times*, (April 4, 2009) http://www.tehrantimes.com/index_View.asp?code=191347 (accessed December 21, 2010).
[256] Cole, Juan. "The Greens in Iran are a Movement, not a Coup," Informed Comment, (June 13, 2010) http://www.juancole.com/2010/06/the-greens-are-a-movement-not-a-coup.html (accessed December 17, 2010).

Ayatollah Khomeini chanting, "Khameini is a murderer and his leadership is void."[257]

ICT in the 2009 Election and Protests

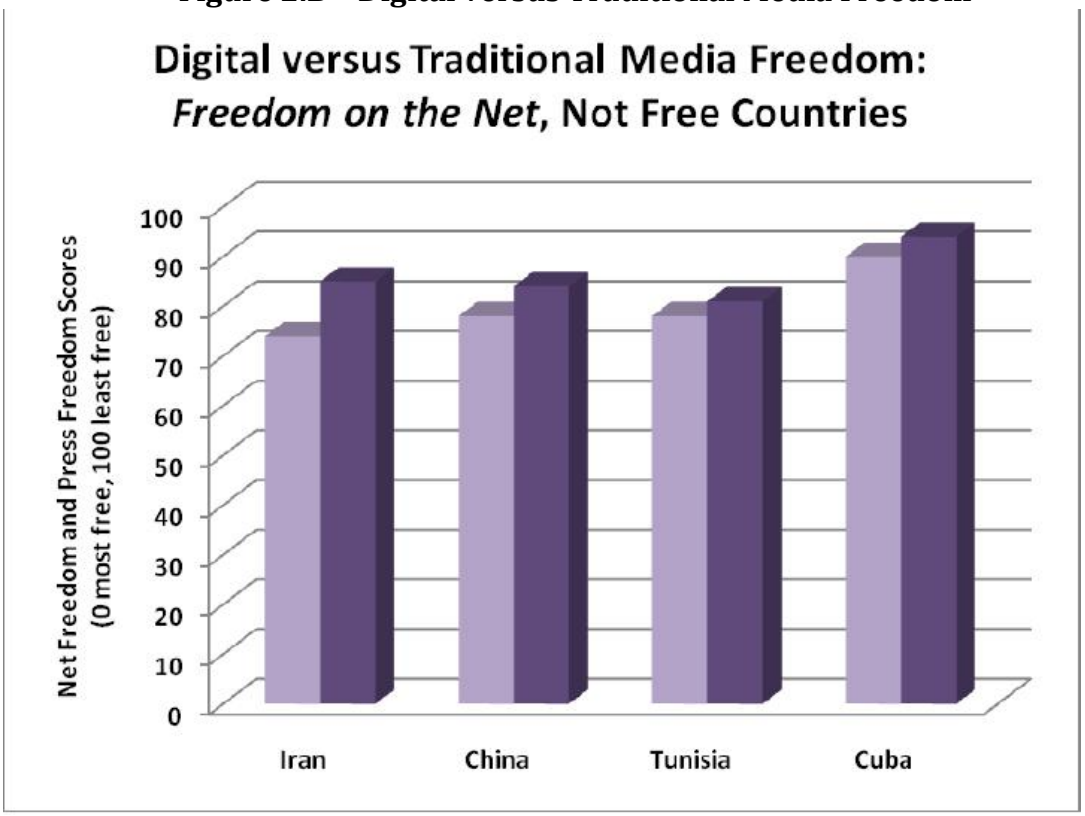
During the 2009 election, Mousavi's green wave supporters and the campaign itself utilized new media tools to build support for Mousavi's candidacy and persuade voters that his policies would lead to a more fruitful and prosperous Iran. He appeared on traditional media outlets like Al Jazeera and in the *Tehran Times*, [258] but he also maintained an active website, Facebook and Twitter pages. His campaign also employed a SMS text messaging campaign to mobilize voters, and created official campaign songs and videos uploaded to YouTube and other digital mediums.[259] [260] [261]

The almost unlimited access to ICT by the Mousavi campaign was due to the fact that he was an official candidate for President, which meant that he was vetted and approved by the Guardian Council. Abbas Milani explains that it would have been nearly impossible for the Council to deny Mousavi the opportunity to run since he had strong revolutionary credentials and was the former Prime Minister during the Iran-Iraq war.[262] Once Ahmadinejad was declared to have won a second term as

[257] Sadjadpour, Karim. "Off the Political Radar," *Qantara*, (2010) http://en.qantara.de/webcom/show_article.php/_c-476/_nr-1343/i.html (accessed December 12, 2010).
[258] Mousavi, Mir Hossein. Campaign Website, http://www.mir-hosseinmousavi.com/policies.html (accessed December 1, 2010).
[259] Szrom, Charlie. "Iran Tracker," American Enterprise Institute, (May 13, 2009) http://www.irantracker.org/tehran/mir-hossein-mousavi-biography-and-campaign-news (accessed December 5, 2010).
[260] "Facebook page of Mousavi," http://www.facebook.com/#!/mousavi (accessed December 5, 2010).
[261] "Twitter page of Mousavi," http://twitter.com/MirTweets (accessed December 5, 2010).
[262] Milani, Abbas. "The Green Movement," United States Institute of Peace, http://iranprimer.usip.org/resource/green-movement (accessed December 5, 2010).

President, the regime quickly squelched the Mousavi camp's unfettered access to the Internet.

Figure 2.B – Digital versus Traditional Media Freedom[263]



Iranian dissidents living in the west have heralded the Internet as serving as a "virtual public square" where Iranian civil society has an outlet for free "cyber" expression.[264] But the picture looks bleaker when viewed up close. Freedom House's initiative, "Freedom on the Net" measures Internet and digital freedom in countries across the globe. Out of 195 countries scored, Iran ranked #181 (tying with China and Rwanda) in Internet and other digital restrictions.[265] Freedom

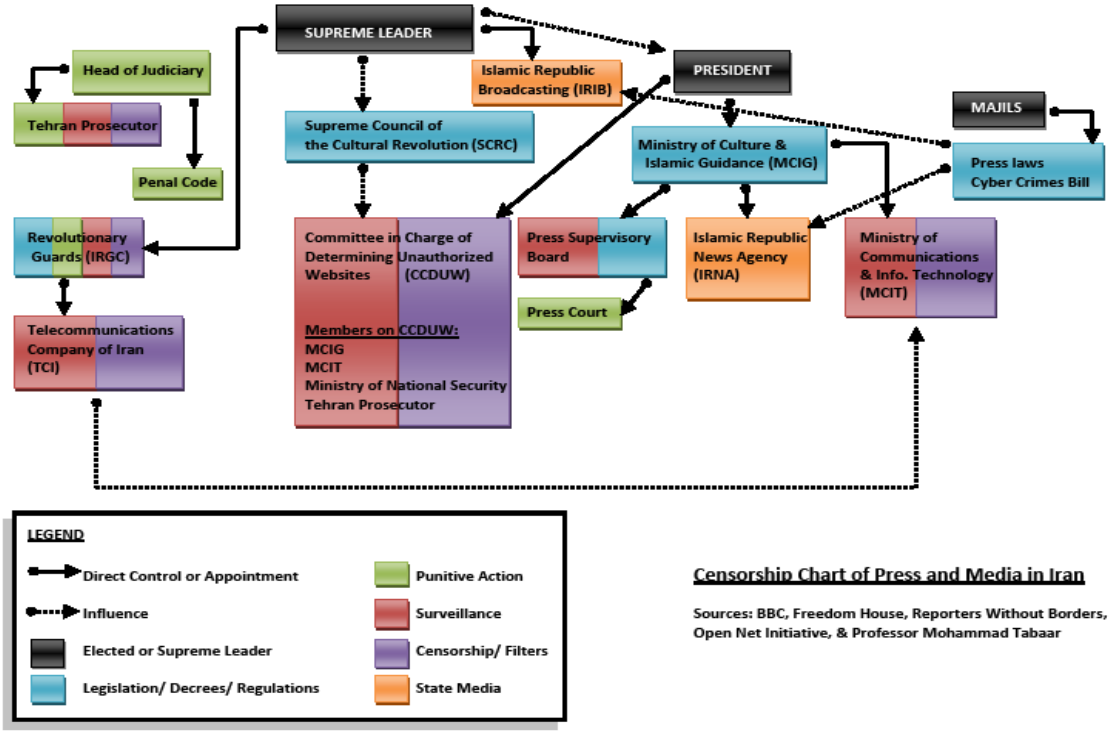
[263] Ibid.
[264] Memarsadeghi, Mariam. "Technology Fund: Investing in the Green Movement for Democracy," International Perspectives on the Middle East (2010): 1.
[265] "Freedom on the Net," Freedom House (2009), 70-75, http://www.freedomhouse.org/template.cfm?page=383&report=79 (accessed July 11, 2010).

House has judged its record of abuses as worse than Syria, Saudi Arabia, Sudan and Pakistan.

The Open Net Initiative has tested the Iranian regime's control mechanisms on the Internet and found Tehran employs one of the world's most sophisticated filtering mechanisms. The pervasive censorship is preventative by blocking predetermined words, phrases or opposition websites. Portals, websites, emails, SMS text messages, and blogs are under constant surveillance and often blocked by an array of bureaucratic monitors. The chart below, created for this paper, illustrates the various levers of control exerted by Iran's Supreme Leader, President, and the *Majlis*.

As complex as the graphic appears, the myriad system of censorship, surveillance, and legal code governing the Internet has at times proved even too byzantine for Iranian watchdogs to manage, allowing hackers and dissidents an inadvertent degree of virtual freedom. As such, some Iranian dissident are in a virtual cat and mouse game with the regime's security forces, constantly trying to stay one step ahead of the latest censorship techniques. This chart does not imply that the regime is unsuccessful at censorship, but rather a pattern has emerged where the security apparatus becomes more brutal when the complicated bureaucracy fails.

Figure 2.C – Censorship Chart of Press and Media in Iran



Conclusion

Even though Iranian dissidents were able to utilize sophisticated communications tools like the Internet, their ability to force a regime change or even fundamental reforms was still very limited due to three factors that are unconnected to the regime itself: First, the Green Movement had no clearly defined political goals. For the movement to maintain cohesion despite the rigid security crackdowns, it needed to be seen as seizing the momentum from the Islamic state. Second, the Green Movement no longer has a "call to action" or unifying message to draw in a diversity of supporters. During the 1979 revolution, Ayatollah Khomeini's genius was his ability to clearly define the goals of the revolution, and have the masses repeat these phrases relentlessly during the protests. As Mohammadi notes, "…the dominant slogan of the movement was *marg bar Shah*, literally "Death to the

Shah."[266] Khomeini's goals during the last revolution were unambiguous; he clearly called for an end to the Pahlavi monarchy and replacement with an Islamic government. The Green Movement fails this test.

Finally, related to the lack of cohesive political goals and messaging was the anemic leadership at the top of the Green Movement. Karim Sadjadpour explains that originally the grassroots and Internet driven aspects of the Green Movement were viewed by leading activists as a more democratic way to manage the movement since they were not relying on one single leader who could be "decapitated" by the regime, causing a major blow to their efforts.[267] While the view of the Internet as a democratizing force that makes traditional organizational dissent obsolete is in keeping with current Internet utopian theorists, it is a strategy that has failed the movement in Iran to date.

As of the writing of this paper[268], the visible protests on a grand scale have now diminished. The movement failed to force a legitimate investigation of the ballot rigging or a new election, but most analysts contend the religious regime has suffered permanent damage its credibility.[269] In August 2009, Mousavi reportedly formed a new group, "The Green Path of Hope" with the goal of organizing the millions who supported him during the Presidential election and then protested in

[266] Sreberny-Mohammadi, Annabelle and Ali Mohammadi, *Small Media, Big Revolution* (Minneapolis: University of Minnesota Press, 1994), 118.
[267] Sadjadpour, Karim. "Off the Political Radar," *Qantara*, (2010) http://en.qantara.de/webcom/show_article.php/_c-476/_nr-1343/i.html (accessed December 12, 2010).
[268] This chapter was completed in December 2010.
[269] Majd, Hooman. "Think Again: Iran's Green Movement," *Foreign Policy*, (January 6, 2010) http://www.foreignpolicy.com/articles/2010/01/06/think_again_irans_green_movement (accessed January 6, 2010).

the streets.[270] His spokesperson, Mohsen Makhmalbaf, explained the movement's reorganizational phase stating they were "…expanding from the big cities to the smaller towns and making connections abroad while sharpening goals and ideas."[271]

Dissident use of ICT in Iran today is characteristic of how other forms of media were employed in of Iran's past. Despite rigid controls, the Internet and mobile phones can provide limited virtual forums for dissent, mobilization and coordination in the absence of physical space. These technologies have also allowed Iranian dissidents to signal their democratic desires to the international community. However, while communications tools have proved an important element in post-modern revolts against authoritarians, history reveals a spotty record of success. The Green Movement and other Iran dissident groups need continued open lines of communication to obtain their desired reforms. In the case of the Internet, continual subversion of the censors will be a challenging feat that forces citizens to constantly outmaneuver the regime. Thus far, despotism and suppression have been highly successful for the state and it appears that "bullets…trump tweets."[272]

[270] Daragahi, Borzou and Ramin Mostaghim, "Mousavi forms new political front," Los Angeles Times, (August 16, 2009) http://articles.latimes.com/2009/aug/16/world/fg-iran-mousavi16 (accessed December 22, 2010).
[271] Ibid.
[272] Kristof, Nicholas. "Tear Down This Cyberwall!" *New York Times*, (June 17, 2009) http://www.nytimes.com/2009/06/18/opinion/18kristof.html (accessed October 13, 2010).

CHAPTER 3 – WMD TERRORISM: NEW MEDIA'S IMPACT ON THE CBRN THREAT

Technological advances in ICT have enabled the exponential growth of access to information in the past two decades. This has created global parity for information gathering among those with access to the Internet, roughly 2.7 billion people or 39% of the world's population.[273] While the second chapter of this thesis explored new media's role in internal state security by examining power differentials between the individual and the state when ICT is utilized, the third chapter will focus on the relationship between violent non-state actors' (VNSA) Internet usage as they operate in opposition to the formal nation state system, otherwise known as an extrastate conflict.

An evaluation of all transnational groups' nefarious behavior as empowered by ICT is too expansive a topic for this paper; instead this chapter will focus on new media's impact on the Chemical, Biological, Radiological and Nuclear (CBRN) terrorism threat. Specifically, this chapter seeks to understand why the al-Qaeda network, despite their committed desire and increased access to information on weapons of mass destruction via the Internet, failed to successfully conduct a single CBRN attack against the United States or its allies in the last decade as predicated by many academic experts and policy makers.

This thesis chapter will test the notional theory that the threat of CBRN terrorism has increased due to the increasingly free flow of information on weapons of mass destruction by presenting an empirical analysis of CBRN datasets. This

[273] International Telecommunication Union, "ICT Facts and Figures." Accessed June 14, 2013. http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf.

paper uses al-Qaeda's unconventional weapons program as a case study to evaluate the phenomenon of ICT and its empowerment of non-state actors. By evaluating prior empirical findings and by presenting new data analysis on CBRN terrorism, this chapter will analyze the present state of al-Qaeda and other jihadists' efforts to accomplish their stated goals of fashioning devices with sufficient lethality to kill millions of Americans, while also seeking to contextualize the significance of new media as a tool that increases motivations and capabilities.

Literature Review

After the attacks of September 11, 2001 (henceforth 9/11), many leading thinkers in the counterterrorism community predicted it would be only a matter of time before a VNSA would successfully attack the United States with a CBRN weapon. In fact, in June 2003 the U.S. government issued a report assessing a "high probability" that al-Qaeda would conduct a weapon of mass destruction attack within the following two years.[274] One of the principal arguments promulgated by security experts after 9/11 was that VNSAs could easily acquire the information on the Internet to build a crude weapon, such as an improvised nuclear device, and detonate it against the United States or its interests abroad. Yet, extremist groups like al-Qaeda have failed to conduct such attacks despite their well-publicized ambitions.

The lack of a mass-casualty post-9/11 terrorist attacks on the American homeland aside, historically CBRN events are a rarity. On average, CBRN terrorist

[274] Mowatt-Larssen, Rolf. "Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality?" Manuscript. Harvard Kennedy School, 2010. http://belfercenter.ksg.harvard.edu/publication/19852/al_qaeda_weapons_of_mass_destruction_threat.html.

attacks are half as lethal as conventional terrorist attacks,[275] and prior to 9/11, no single conventional terrorist attack killed more than 500 people.[276] In the twentieth century, only fourteen terrorist events have killed more than 100 people, and all of those events used conventional modes.[277] Despite the fatality disparity between conventional and unconventional weapons outcomes, the fact remains that successful deployment of a CBRN device could precipitate "mass panic and large-scale economic disruption" that goes beyond the number of causalities associated with the attack.[278] Accordingly, if new media aids al-Qaeda and likeminded groups in the fabrication of CBRN capabilities, as some have postulated, then careful study is warranted.

Defining WMD

In discussing CBRN weapons and how one might use new media to acquire the information for building a crude device, some technical parameters must be established.

Only one weapon type, nuclear, poses an existential threat to a state and is therefore classified as a weapon of mass destruction. Chemical, biological and radiological weapons are more accurately characterized as Weapons of Mass Disruption

[275] Ivanova, Kate, and Todd Sandler. 2007. CBRN attack perpetrators: An empirical study. Foreign Policy Analysis 3 (4) (10/01): 273.
[276] Hoffman, Bruce. "CBRN Terrorism Post 9/11," in Weapons of Mass Destruction and Terrorism, eds. Russell D. Howard and James Forest (New York: McGraw-Hill, 2007).
[277] Kazi, Reshmi. 2011. The correlation between non-state actors and weapons of mass destruction. Connections (18121098) 10 (4) (09/01): 1.
[278] Blair, Charles. "Radiological Ray Gun: More Buck Rogers Fantasy than Risk to Real People." FAS Strategic Security Blog (blog), June 20, 2013. http://blogs.fas.org/security/2013/06/radiological-ray-gun-more-buck-rogers-fantasy-than-risk-to-real-people/ (accessed July 3, 2013).

(WMD).[279] [280] [281] This is because nuclear weapons are the only CBRN type capable of creating a destructive mass-casualty scenario, whereas chemical, biological, and radiological devices are unlikely to produce multitudinous deaths due to significant weaponization and dispersal limitations, especially when employed by a non-state entity.[282]

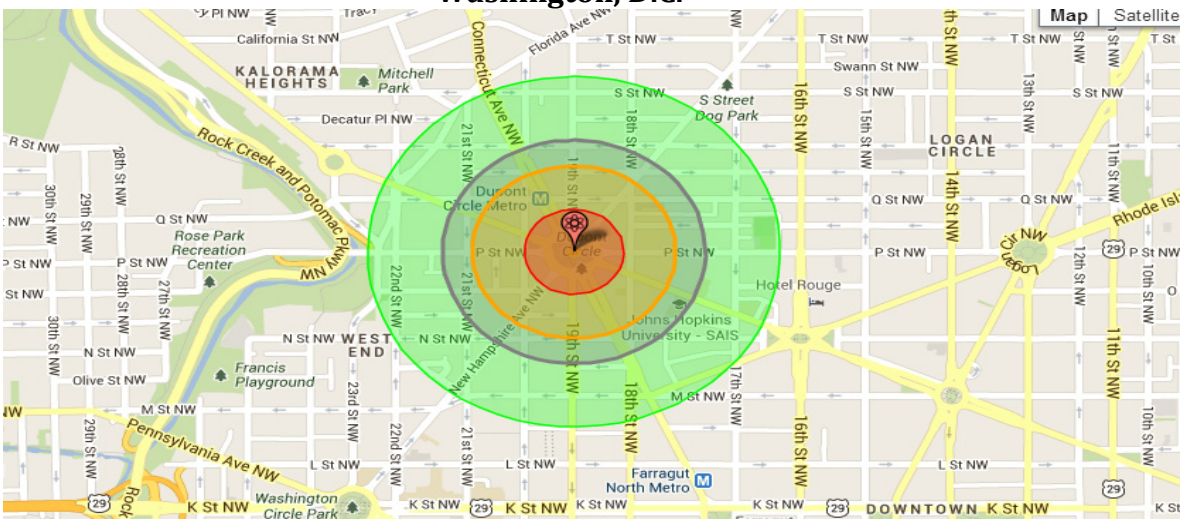
Conversely, a "dirty bomb," better classified as a radiological dispersion device (RDD), would not produce mass casualties since the radiological sources available to VNSAs do not contain enough radioactive material to cause significant harm.[283] Persons in proximity to an RDD explosion are more likely to die from the blast effects than from exposure to the dispersed radioisotopes. In addition, highly radioactive sources, such as gamma emitters, are very difficult to handle and exposure to the ionizing radiation during creation of the RDD could be lethal.[284]

Figure 3.A contains a computer simulation model of the hypothetical blast radius from a crude 100 ton nuclear device employed by a terrorist. This simulation shows that nuclear device detonated at Dupont Circe in Washington, D.C. under clear atmospheric conditions would have lethal radiation radius (colored green) stretching from Rock Creek Parkway to 16th Street Northwest, encompassing the Johns Hopkins D.C. campus, approximately three-quarters of one mile in

[279] Macfarlane, Allison. "All Weapons of Mass Destruction Are Not Equal," Audit of the Conventional Wisdom Series, Center for International Studies, MIT. July 2005.
[280] Kelly, Henry, and Michael Levi. Federation of American Scientists, "Weapons of Mass Disruption." Last modified November 2002. Accessed August 5, 2013. http://www.fas.org/ssp/docs/021000-sciam.pdf.
[281] For the purposes of this paper, henceforth WMD will refer to weapons of mass disruption, as defined above.
[282] Blair, Charles. "Radiological Ray Gun: More Buck Rogers Fantasy than Risk to Real People." FAS Strategic Security Blog (blog), June 20, 2013. http://blogs.fas.org/security/2013/06/radiological-ray-gun-more-buck-rogers-fantasy-than-risk-to-real-people/ (accessed July 3, 2013).
[283] Ibid.
[284] Ibid.

diameter.[285] Using the Nuclear Weapons Archive's estimation for short-term fatalities by counting every person in the 5 psi blast overpressure contour around the hypocenter, a 100 ton nuclear detonation in Dupont Circle could kill approximately 17,600 people.[286] [287] Contrast Figure 3.A's mortality estimates to those from the Japanese apocalyptic cult Aum Shinrikyo's March 20, 1995 chemical weapons (CW) attack on the Tokyo subway: using liquid sarin (a nerve agent) in plastic bags, Aum cult members punctured the bags with sharpened umbrella tips, releasing liquid and fumes that killed 13 people and sent 6,000 to the hospital with injuries, many psychological.[288]

Figure 3.A – Hypothetical Blast Radius of a Crude Nuclear Weapon in Washington, D.C. [289]



[285] Wellerstein, Alex. Nukemap (blog), http://nuclearsecrecy.com/nukemap/ (accessed June 3, 2013).
[286] Sublette, Carey. "Section 5.0 Effects of Nuclear Explosions." Nuclear Weapons Archive (blog), May 15, 1997. http://nuclearweaponarchive.org/Nwfaq/Nfaq5.html (accessed June 5, 2013).
[287] Dupont Circle region and surrounding areas have a population density of approximately 40,000 persons/sq. mile according to Census Tract, 2010 Population, Housing Units, Occupancy Rate, and Average Household Size data retrieved from the U.S. Census Bureau. Available athttp://factfinder2.census.gov. With a blast radius of .44 square miles, estimated fatalities from such a device would be approximately 17,600 persons.
[288] "Aum Shinrikyo: Insights Into How Terrorists Develops Biological and Chemical Weapons." Manuscript. CNAS, 2012. http://www.cnas.org/files/documents/publications/CNAS_AumShinrikyo_SecondEdition_English.pdf.
[289] Wellerstein, Alex. Nukemap (blog), http://nuclearsecrecy.com/nukemap/ (accessed June 3, 2013).

The Aum Shinrikyo sarin attack is one of the most successful uses of CW by any VNSA in history, but resulted in relatively few deaths. Aum Shinrikyo had capabilities and advantages that gave it access to chemicals and agents, production facilities, testing venues, and free range of movement, of which most post-9/11 apocalyptic groups do not have at their disposal. This included highly skilled members, plenty of money, relative freedom of movement, and multiple disguised factories for mass production of agents. A United Nations report estimated that one of Aum's production facilities, the Satyan 7 building, and its contents cost $30 million.[290] Chemical, biological and radiological weapons pale in lethality compared to the potential catastrophic devastation of a successfully deployed nuclear device.

Experts on CBRN Terrorism

The study of CBRN terrorism as a separate phenomenon from conventional attacks is an important part of the literature on terrorism research, even though these types of attacks have been comparatively rare. "The single most important national security threat we face is nuclear weapons falling into the hands of terrorists," proclaimed then-Presidential candidate Barak Obama in a campaign video from 2008.[291] According to prominent terrorism expert Gary Ackerman, a successful detonation of a CBRN device could yield "inordinate psychological and social impact," as well as onerous cleanup costs, long-term property damage, loss of

[290] ibid.

[291] Mooney, Alexander. "CNN Politics." Obama promotes foreign policy cred in new ad (blog), July 15, 2008. http://politicalticker.blogs.cnn.com/2008/07/15/obama-promotes-foreign-policy-cred-in-new-ad/ (accessed March 5, 2013).

commerce, and more importantly the catastrophic loss of life from a nuclear weapon.[292] [293]

As such, it is reasonable to be alarmed by al-Qaeda and other extremist groups' spread of technical manuals offering advice on creating CBRN devices as well as the religious justification to use them. New media mogul Tina Brown lamented that the "conjunction of 21st-century Internet speed and 12th-century fanaticism has turned our world into a tinderbox."[294] Moreover, terrorism experts since 9/11 have routinely viewed new media's dissemination of information on CBRN weaponization as one of the casual factors related to the alleged increased WMD terrorism threat. [295] [296] These experts contend that ICT's pervasive spread of knowledge on CBRN is problematic, especially when coupled with the globalization of Internet commerce, which allows amateur scientists to purchase Do-It-Yourself labs and tinker with dangerous dual-use technologies.[297] [298]

While the "diffusion of knowledge" on unconventional weapons via the Internet is disquieting, respected terrorism expert Bruce Hoffman detailed in his 2002 Congressional testimony that it was the Internet's rapid spread of radical

---

[292] Ivanova, Kate, and Todd Sandler. 2007. CBRN attack perpetrators: An empirical study. Foreign Policy Analysis 3 (4) (10/01): 273.
[293] Ackerman, Gary. Introduction. Jihadists and Weapons of Mass Destruction. Edited by Gary Ackerman and Jeremy Tamsett. Boca Raton, FL: CRC Press, 2009. pp. xi-xxxiii.
[294] Brown, Tina. "Death by Error." May 19, 2005. http://www.washingtonpost.com/wp-dyn/content/article/2005/05/18/AR2005051802083.html (accessed July 1, 2013).
[295] Forest, James, and Sammy Salama. Jihadist Tactics and Targeting. Jihadists and Weapons of Mass Destruction. Edited by Gary Ackerman and Jeremy Tamsett. Boc: CRC Press, 2009.
[296] Kazi, Reshmi. 2011. The correlation between non-state actors and weapons of mass destruction. Connections (18121098) 10 (4) (09/01): 1.
[297] Federation of American Scientists, "Case Studies in Dual Use Biological Research." Accessed March 14, 2013. http://www.fas.org/biosecurity/education/dualuse/index.html.
[298] Hessel, Andrew, Marc Goodman, and Steven Kotler. 2012. Hacking the President's DNA. Atlantic Monthly (10727825) 310 (4) (11/01): 82.

ideology that was far more deleterious. "As one U.S. government observer of the terrorism Internet phenomenon has noted in the context of the radical Islamic web sites, 'never in history has there been an opportunity where propaganda is so effective.' " [299] [300] New media could also theoretically drive groups like a-Qaeda to pursue CBRN proficiency, since terrorists may feel the need to "raise the bar" by executing attacks even more spectacular than 9/11, thus garnering greater attention to their *raison d'être*.[301]

The fear over CBRN terrorism has saturated the public as well. Brian Jenkins's Congressional testimony from his 2008 book, "Will Terrorists Go Nuclear?" cites public opinion polls showing that 40% of Americans believe that a nuclear terrorist event would happen by 2013. This contrasts starkly with one European nuclear scientist's estimate of the likelihood of a nuclear terrorist attack at 1%.[302] The reason for the vast discrepancies between what elected officials and the populace purport as an imminent threat, and nuclear scientists assess to be only marginal, is the lack of sophisticated statistical analysis against salient CBRN data, according to Ackerman.[303] After a review of 120 scholarly works on CBRN

[299] Hoffman, Bruce. "CBRN Terrorism Post 9/11," in Weapons of Mass Destruction and Terrorism, eds. Russell D. Howard and James Forest (New York: McGraw-Hill, 2007).
[300] Militant Islamic Political Activism on the Worldwide Web, Foreign Broadcast Information Service, "RAND." Last modified December 19, 2000. Accessed August 5, 2013. http://130.203.133.150/showciting;jsessionid=1F0207FB4B21FF92EEE26C53ADD49CC7?cid=13454017.
[301] Ivanova, Kate, and Todd Sadler. "CBRN Incidents: Political Regimes, Perpetrators and Targets." Terrorism and Political Violence. No. 3 (2006): pp. 423-448.
[302] Leitenberg, Milton. 2009. The threat of bioterrorism, real and imagined. World Politics Review (19446284) (10/27): 5.
[303] Asal, Victor H., Gary A. Ackerman, and R. K. Rethemeyer. 2012. Connections can be toxic: Terrorist organizational factors and the pursuit of CBRN weapons. Studies in Conflict & Terrorism 35 (3) (03/01): 229.

terrorism, Ackerman concluded that CBRN threat assessments were largely based on "anecdotal evidence provided by a handful of prominent cases."[304]

Other security experts assess that 9/11 was an outlier event and since a CBRN terror event is even less likely to occur, they see little value in the consternation over al-Qaeda's WMD attempts.[305] Leading bioterror pessimist Milton Leitenburg points out the technical challenges in carrying out CBRN attacks, noting that "bioterrorism killed no U.S citizens in the twentieth century and five to date in the twenty-first century," a reference to the 2001 "Amerithrax" attacks. [306] Still other experts contend that there are sometimes greater incentives for groups *not* to pursue WMD capabilities since actually detonating such weapons could result in a group losing support and funding from their targeted constituencies. Such attacks could also invite a massive retaliatory response by the aggrieved state, which could destroy the VNSA or the host country, akin to the U.S. invasion of Afghanistan after 9/11.[307] [308]

Evaluation of Prior Empirical Research

In the field of CBRN terrorism study, three prominent empirical studies[309] quantitatively test the hypothesized casual factors of VNSA pursuit of CBRN against the Monterey Institutes' Weapons of Mass Destruction database (hereafter Monterey WMD database), which documents all open-source CBRN incidents and is

[304] Ibid.
[305] Leitenberg, Milton. 2009. The threat of bioterrorism, real and imagined. World Politics Review (19446284) (10/27).
[306] Ibid.
[307] Ivanova, Kate, and Todd Sadler. "CBRN Incidents: Political Regimes, Perpetrators and Targets." Terrorism and Political Violence. No. 3 (2006): pp. 423-448.
[308] Ackerman, Gary, and Laura Snyder. 2002. Would they if they could? Bulletin of the Atomic Scientists 58 (3) (05/01): 40.
[309] This data point is accurate as of summer 2013, when this chapter was completed.

one of the most respected datasets in the field of WMD research. These studies include Kate Ivanova and Todd Sandler's 2006 and 2007 research "CBRN Incidents: Political Regimes, Perpetrators, and Targets" and "CBRN Attack Perpetrators: An Empirical Study," respectively. The third is "Connections Can Be Toxic: Terrorist Organizational Factors and the Pursuit of CBRN Terrorism" by Gary Ackerman, Victor Asal, and R. Karl Rethemeyer. Of note, Ackerman, Asal and Rethemeyer's research slightly deviates by merging the Monterey WMD database with datasets from the Memorial Institute for the Prevention of Terrorism (MIPT) in their statistical analysis.

Of the three research analyses, only Ackerman and his colleagues test CBRN terrorism incidents against technological and communications development in the VNSA's host nations. Despite the claims from policy makers, academics, and elected officials that the dissemination of CBRN knowledge will lead to more attacks, the other two studies do not test new media theories as it relates to casual factors in VNSA use of CBRN. Ivanova and Sandler's studies lightly reference a greater "knowledge base" in democracies, but that is in regards to the increased access to skilled technical experts and universities in democracies, not ICT.[310]

The Ackerman study uses quantitative methods to evaluate CBRN incidents and VNSA organizational data from 1998 to 2005, whereas the Ivanova and Sandler studies query similar datasets from 1988 to 2004 due to the rarity of CBRN attacks before 1988, resulting in limited variation in CBRN events to explain using

[310] Ivanova, Kate, and Todd Sandler. 2007. CBRN attack perpetrators: An empirical study. Foreign Policy Analysis 3 (4) (10/01): 273.

inferential statistics.[311] Ivanova and Sandler's 2007 research reveals that per incident, chemical agent use or acquisition by a VNSA is by far the most the most prevalent, followed by biological, radiological, and nuclear attempts. The authors note that the eight documented VNSA nuclear attempts involved al-Qaeda's efforts to acquire enriched uranium with hopes of developing a crude nuclear device, and Chechen rebels' efforts to procure a "suitcase bomb" from ex-Soviet facilities.[312] None of those attempts were successful, according to available open source literature. As noted in the above, the use of the Monterey WMD database starting in 1988 was because of the exponential increase in VNSA use and procurement incidents after 1988; however, the study does not provide any explanation as to why there was such an increase after the late 1980s.

Of the 12 hypotheses presented in the Ackerman study, this paper is most concerned with hypothesis number two: "The higher the level of technological development (as proxied by energy consumption) in the organization's host country, the greater the likelihood of pursuing a CBRN capability."[313] The authors postulate that it is not just access to the Internet, but the ability to collaborate with technical experts from universities, as well as the proliferation of dual-use technologies, which inform VNSA awareness of the potential for WMD. They argue that CBRN knowledge must be merged with substantive institutions since sophisticated understanding of physics, biology and chemistry is necessary for

[311] Ibid.
[312] Ibid.
[313] Asal, Victor H., Gary A. Ackerman, and R. K. Rethemeyer. 2012. Connections can be toxic: Terrorist organizational factors and the pursuit of CBRN weapons. Studies in Conflict & Terrorism 35 (3) (03/01): 229.

weaponization of selected agents. Therefore, integration of the terrorist organization's home country into the global economy through trade is an essential factor for the terrorist CBRN threat.[314]

Of note, the scope of the Ackerman study is defined by exploring the motivations of groups who decide to pursue CBRN. Therefore, hypothesis two is framed by how technological development in the host country may impact VNSA *desires* to pursue CBRN capabilities. The researchers ran 395 observations of organizations' attempts to acquire or actual usage of CBRN from 1998 to 2005 against the United Nations' Conference on Trade and Development (UNCTAD) information and communication index, and 312 observations against the UNCTAD's technology development index. Ackerman and his colleagues found no correlation between the host country's technology development and CBRN terrorism incidents. Neither of the UNCTAD's indexes showed any "statistically significant predictors of CBRN pursuit or use." [315] However, the authors assume that the defeat of their hypothesis may be due to ICT data being immersed in the "economic embeddedness effect," which is their hypothesis that a host country's integration into the global economy makes a VNSA more likely to pursue CBRN weapons, a theory that was consistent across the Ackerman team's models.[316]

While the authors' assumption of ICT availability for countries with economic interdependence may appear on the surface to be reasonable, it is not an assumption that can be taken for granted. Many countries engage in international

[314] Ibid.
[315] Ibid.
[316] Ibid.

trade while limiting Internet access. Indeed, many countries in which al-Qaeda is strongest are led by authoritarian regimes that engage economically with international partners while seeking to limit public access to ICT and freedom of use.

Data Results

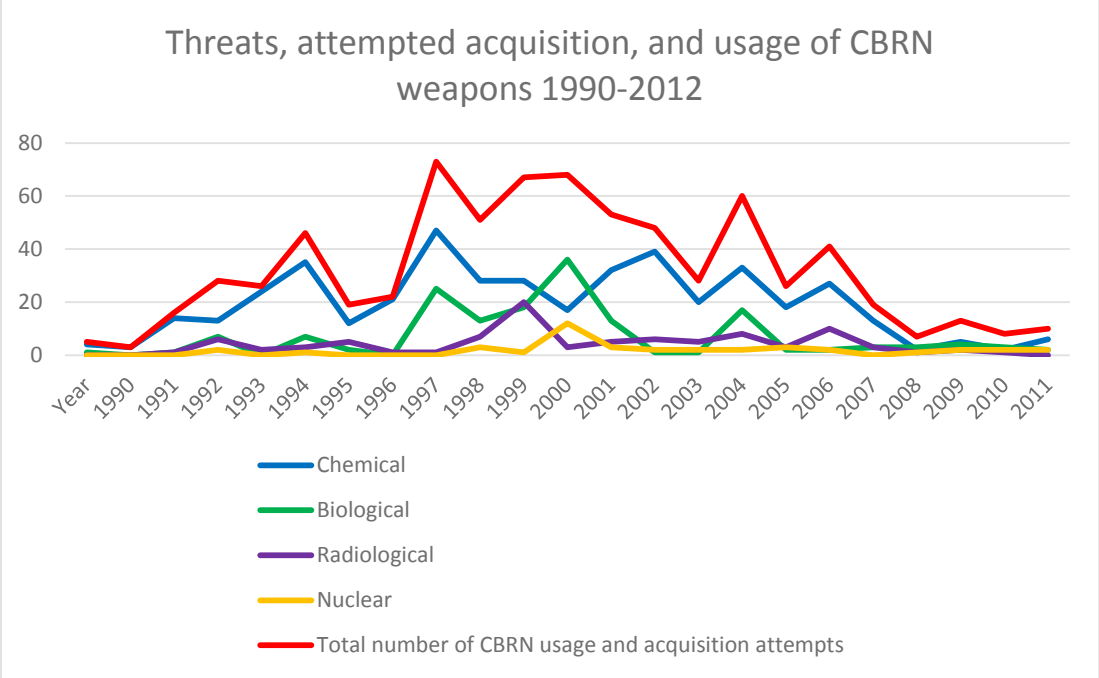
To ascertain whether information diffusion via ICT has had a demonstrable effect on CBRN incidents by VNSAs, this paper applies the Monterey WMB database to the United Nations' International Telecommunications Union (ITU) data on global Internet penetration.[317] All CBRN incidents labeled as a hoax or prank were culled from the data. However, unlike the earlier studies previously referenced, all other acquisition categories were retained in the dataset including those events labeled as "use of agent", "attempted acquisition", "threat with possession", "threat only", "plot only", "possession only", and "unknown."[318] This study incorporates all non-state actor cases, including those tied to criminal networks, since the line between criminality and terrorism is often blurred. For example, criminal syndicates are often intertwined with terrorist organizations in places like Afghanistan and Somalia, where narcotics traffickers and pirates have lent direct financial support and facilitation of weapons to VNSAs.[319] [320] Additionally, "threats only" and "plots only" incidents where agent possession was not publicly substantiated were also

[317] International Telecommunication Union, "ICT Facts and Figures." Accessed June 14, 2013. http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf.
[318] Monterey WMD Terrorism Database. http://wmddb.miis.edu/ (accessed July 2, 2013).
[319] Felbab-Brown, Vanda. Brookings Institute, "U.S. Counternarcotics Strategy in Afghanistan." Last modified October 21, 2009. Accessed April 17, 2013. http://www.brookings.edu/research/testimony/2009/10/21-counternarcotics-felbabbrown.
[320] Cohn, Julie. "Terrorism Havens: Somalia." Council on Foreign (blog), June 20, 2010. http://www.cfr.org/somalia/terrorism-havens-somalia/p9366 (accessed July 28, 2013).

retained, since this paper is concerned not only with how new media might aid in technical knowledge for weapons fabrication, but also if the Internet's diffusion of propaganda persuades more groups to seek a WMD capability.

Figure 3.B provides an annual visualization of all CBRN incidents from 1990 to 2012, and Figure 3.C compares the same total incident data with the global Internet penetration statistics as documented by the ITU. The date parameters were selected because very few CBRN cases were documented prior to 1990, and the Internet was virtually nonexistent prior to this date, rendering the earlier time frames statistically irrelevant. Furthermore, the latter dates coincide with the rise of global ICT usage, which allows for a more relevant comparison with the Internet saturation rates.

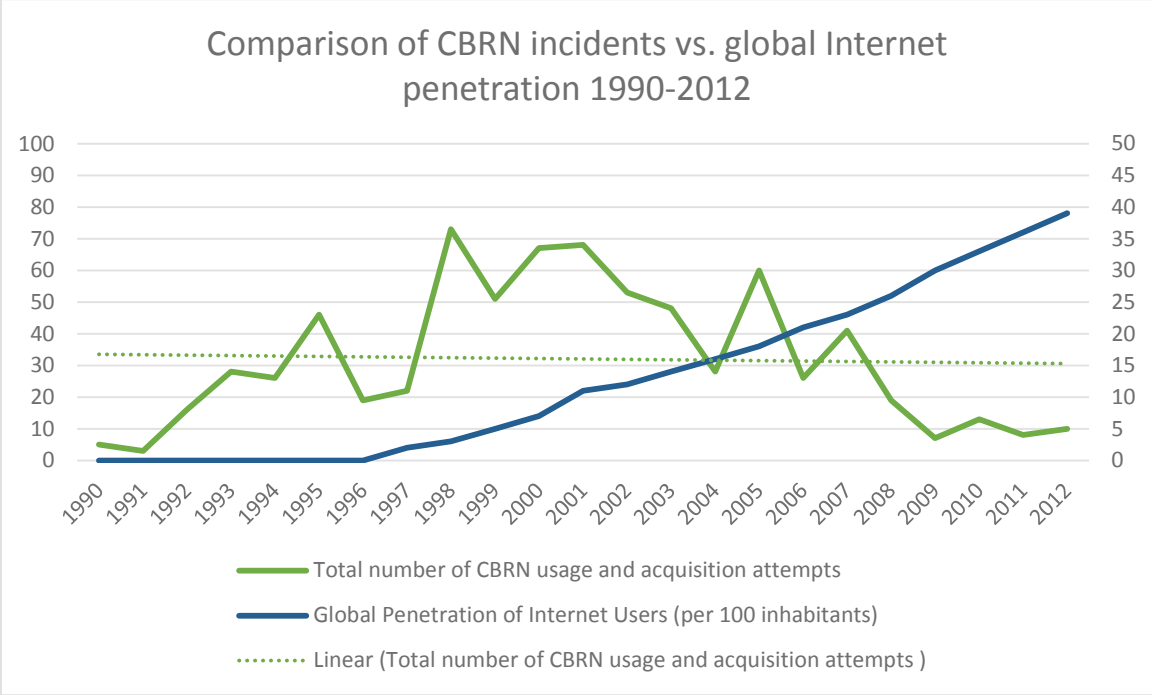
Figure 3.B – Threats, Attempted Acquisition, and Usage of CBRN Weapons [321]



[321] Monterey WMD Terrorism Database. http://wmddb.miis.edu/ (accessed July 2, 2013).

As observed in Figure 3.C, the total CBRN linear trend line is slightly decreasing over the time plotted, but is probably more prudently classified as flat due to the small-*n* sample size of the available data. As global Internet users continue a steep upward trend, the data does not show a long-term correlation between CBRN incidents and Internet usage. CBRN incidents rose in the late-1990s before falling in the late 2000s.

Figure 3.C – Comparison of CBRN incidents versus Global Internet Penetration[322] [323]



More importantly, the number of attempted nuclear incidents has remained negligible, with the exception of a small spike in 2000-2001. Since all four variables experienced their highest event rates in the late 1990s and early 2000s, one could hypothesize that apocalyptic VNSAs seeking CBRN weapons may have used ICT to

[322] Ibid.
[323] International Telecommunication Union, "ICT Facts and Figures." Accessed June 14, 2013. http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf.

gain access to greater amounts of information on WMD technologies or radical propaganda encouraging CBRN, than was previously at their disposal. Therefore, their newfound awareness increased the attempted acquisitions and uses.

This conclusion is open for criticism since the Monterey WMB database, like all other open source datasets on CBRN terrorism, is reliant on partial information reported by news organizations, academic studies, or government reports. It could be that the increase in communication technologies biased the data, since theoretically more incidents could be reported than was previously possible. However, this critique does not explain the substantial decrease of events for all variables post 2008, with the subsequent return to early 1990s CBRN incidents levels.

The data does not lend itself readily to determinations of causality. However, it does not appear the reason for the reduction in CBRN events is tied to a VNSA decision to cease pursuit of such weapons. Further, following 9/11, governments adopted significantly more robust counter-terrorism policies and increased ICT monitoring, in essence using the Internet as a tool against VNSAs. These efforts may have undermined the range of VNSA plans, including CBRN attack plots. If this is the case, it would indicate that availability of ICT is a secondary factor in determining the likelihood of VNSAs successfully executing CBRN attacks; the strength of global counter-terrorism efforts appear more relevant, as this factor will determine the space and time that VNSA groups will have to plan, prepare, and execute CBRN attacks.

Case Study: Al-Qaeda and WMD

The paucity of open source data available on VNSA acquisitions makes it nearly impossible to do purely empirical analysis due to the absence of any real WMD attacks.[324] [325] Forecasting human behavior is always challenging, but imperfect datasets provide an important opening for thoughtful consideration of noteworthy CBRN case studies. Publicly-available sources, detainee reports, media documents, press interviews, and a large body of circumstantial evidence clearly indicate that al-Qaeda was just as committed to manufacturing a WMD program as it was to executing the 9/11 attacks.[326]

Al-Qaeda leaders colluded with corrupt states and its Islamist allies over four continents for a decade to systematically procure the knowledge and materiel necessary to create a WMD program with emphasis on nuclear and biological weapons.[327] [328] Osama bin Laden's vision for the potential devastation of CBRN weapons combined with deputy Ayman al- Zawahiri's programmatic administration to propel al-Qaeda forward in its pursuits. Pivotal to those efforts was al-Qaeda's use of ICT to propagate the religious justification to conduct said attacks, to gather

[324] Kazi, Reshmi. 2011. The correlation between non-state actors and weapons of mass destruction. Connections (18121098) 10 (4) (09/01): 1.

[325] Of course, Kazi's argument is dependent on what one classifies as CBRN terrorism. Even so, there are still only handfuls of actual CBRN events with which one can explore.

[326] Mowatt-Larssen, Rolf. "Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality?" Manuscript. Harvard Kennedy School, 2010. http://belfercenter.ksg.harvard.edu/publication/19852/al_qaeda_weapons_of_mass_destruction_threat.html.

[327] Forest, James, and Sammy Salama. Jihadist Tactics and Targeting. Jihadists and Weapons of Mass Destruction. Edited by Gary Ackerman and Jeremy Tamsett. Boc: CRC Press, 2009.

[328] Center for Nonproliferation Studies, "Chart: Al-Qa`ida's WMD Activities." Last modified May 13, 2005. Accessed June 5, 2013. http://cns.miis.edu/other/sjm_cht.htm.

knowledge on WMD, communicate with technical experts, coordinate attack planning, and provide virtual training to would-be jihadists.[329] [330]

Al-Qaeda's early adaptation of new media tools certainly bestowed an advantage over less tech savvy jihadi groups. However, it seems clear that other factors such as a supportive host nation, freedom of movement, access to skilled technicians, and plentiful financial resources were ultimately more important for CBRN acquisition than the benefits the Internet afforded. Ironically, after 9/11, the Internet is what saved the group from extinction, allowing bin Laden's fantasy of a significant CBRN attack against the United States to survive as a threat, albeit a far less substantial one.

Brief History

Al-Qaeda's WMD machinations reach back 20 years: the operatives under the leadership of Ramzi Yousef conducted the 1993 World Trade Center (WTC) bombing had attempted to incorporate sodium cyanide into their homemade bomb to generate deadly hydrogen cyanide gas, which could have resulted in a much larger death toll.[331] The judge in Yousef's case stated on the record that the sodium cyanide burned in the blast rather than vaporizing to make hydrogen cyanide. There appears to be some contention around this issue, as then a senior research associate with the Center for Nonproliferation Studies, John Parachini, thoroughly examined the public court documents on the first WTC bombings and concluded that the WTC

[329] Hoffman, Bruce. RAND, "Congressional Testimony: The Use of the Internet by Islamic Extremists." Last modified May 2006. Accessed June 17, 2013. http://www.rand.org/content/dam/rand/pubs/testimonies/2006/RAND_CT262-1.pdf.

[330] Forest, James, and Sammy Salama. Jihadist Tactics and Targeting. Jihadists and Weapons of Mass Destruction. Edited by Gary Ackerman and Jeremy Tamsett. Boc: CRC Press, 2009.

[331] "The World Trade Center Bombers," in Jonathan B. Tucker, ed., Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons (Cambridge, MA: MIT Press, 2000), pp.185-206.

bombers did not use a chemical poison, but only considered it as an option.[332] Of course, there is the possibility that the sealed findings, which the judge was privy to, offered evidence not in the public record.[333] Further, it seems unlikely that the judge would have fabricated the evidence he cited, lending credence to the assertion that the WTC bombers attempted to use a chemical device.

The actual first confirmation of bin Laden's desire to procure CBRN weapons came in late 1993 when al-Qaeda allegedly purchased uranium in Sudan for $1.5 million possibly with help from former Sudanese President Saleh Mobruk, according to the testimony of a FBI informant.[334] After the 1998 merger of Zawahiri's Egyptian Islamic Jihad with al-Qaeda, Zawahiri oversaw the strategic biological and nuclear weapons procurement processes. Throughout the 1990s and early 2000s, al-Qaeda endeavored to obtain CBRN weapons through "parallel paths" via multiple network nodes.[335] Moving independently, each unit adhered to tight compartmentalization and reported directly to al-Qaeda leaders regarding its progress to buy, steal, or manufacture WMD.[336] This strict command and control of weapons acquisition was thwarted after the United States' invasion of Afghanistan, which scattered the leadership and destroyed its ability to function in the smooth hierarchical fashion as it once had. This supports the assertion that while ICT have facilitated VNSA

[332] Ibid. 205
[333] Ibid. 200
[334] Mowatt-Larssen, Rolf. "Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality?" Manuscript. Harvard Kennedy School, 2010. http://belfercenter.ksg.harvard.edu/publication/19852/al_qaeda_weapons_of_mass_destruction_threat.html.
[335] Ibid.
[336] Ibid.

attempts to procure CBRN, it remains a secondary factor in comparison to the efforts of state counter-terrorism programs.

Weapons on the Web

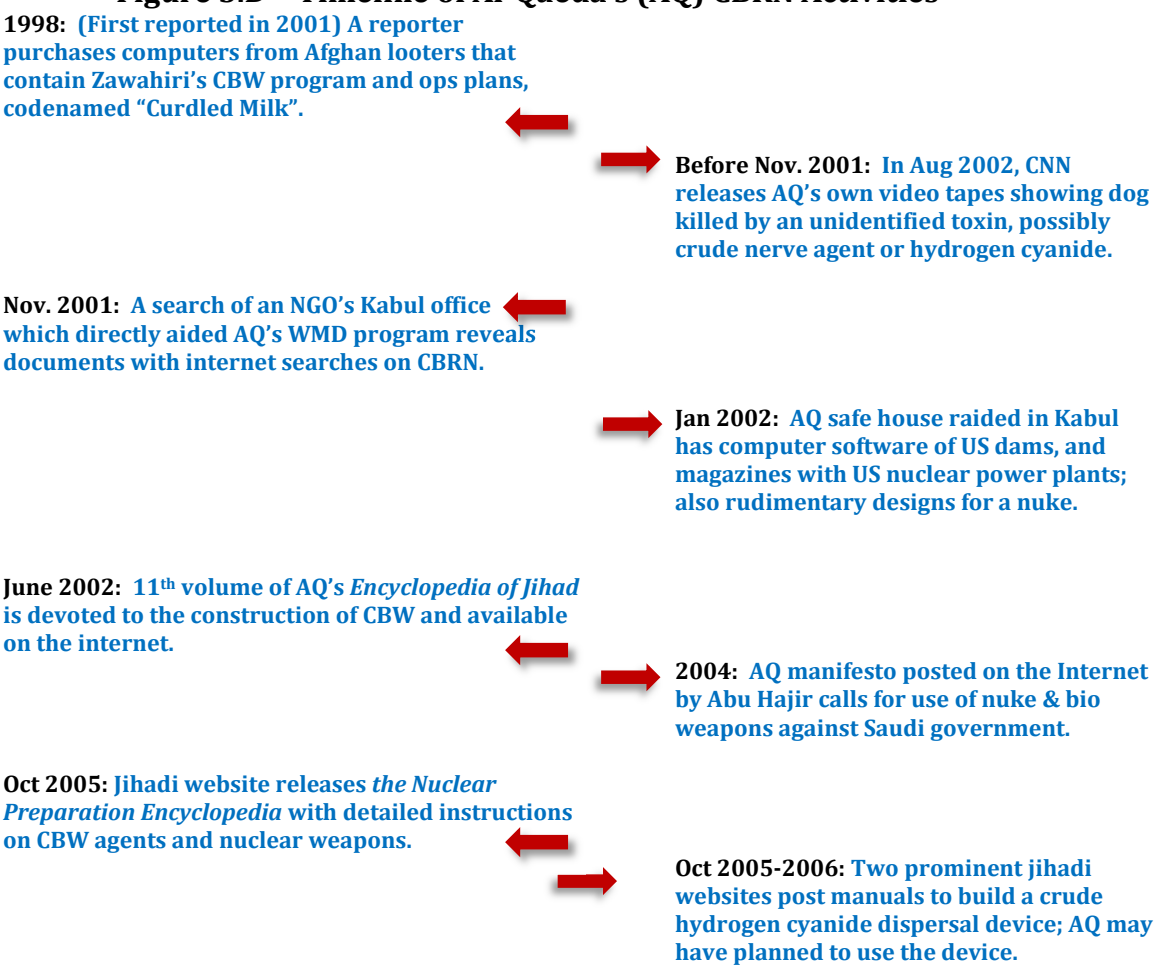
Rather than directly facilitating VNSA pursuit of CBRN, ICT appears far more relevant in enabling VNSA survival by facilitating propaganda. As VNSAs like al-Qaeda continue to harbor the same aspirations for mass casualty attacks, ICT's primary contribution is in enabling the survival of an ideology that might otherwise have been extinguished. Professor Bruce Hoffman described how al-Qaeda even before 9/11 placed an emphasis on external communications by recruiting Egyptian computer experts to create an extensive network of websites and e-mail capabilities that continue to function today despite the group's ouster from Afghanistan.[337] Hoffman contends that al-Qaeda early on uniquely understood the value of new media, and after it was forced to flee its sanctuary after 9/11, group members utilized the Internet as a "virtual sanctuary" for propaganda, fundraising, terrorist instructional training, and operational planning through email correspondence and web forums.[338]

Of the estimated 4,600 radical Islamist websites as of 2006, only a fraction deals with CRBN terrorism.[339] As Figure 3D demonstrates, al-Qaeda was actively using new media technologies to gather technical details on WMD and potential targets, while also using those same tools to disseminate to jihadi sympathizers the

[337] Hoffman, Bruce. RAND, "Congressional Testimony: The Use of the Internet by Islamic Extremists." Last modified May 2006. Accessed June 17, 2013. http://www.rand.org/content/dam/rand/pubs/testimonies/2006/RAND_CT262-1.pdf.
[338] Ibid.
[339] Forest, James, and Sammy Salama. Jihadist Tactics and Targeting. Jihadists and Weapons of Mass Destruction. Edited by Gary Ackerman and Jeremy Tamsett. Boc: CRC Press, 2009.

knowledge gained on how to conduct an asymmetrical attack. It is difficult to know how many al-Qaeda acolytes and self-radicalizers have viewed their CBRN instructional documents, but according to a *Sunday Times* report, when al-Qaeda's *Nuclear Preparation Encyclopedia* went live on *al-Fardaws'* website in October 2005 it drew over 57,000 visitors.[340]

Figure 3.D – Timeline of Al-Qaeda's (AQ) CBRN Activities[341] [342] [343]



[340] Ibid.
[341] Center for Nonproliferation Studies, "Chart: Al-Qa`ida's WMD Activities." Last modified May 13, 2005. Accessed June 5, 2013. http://cns.miis.edu/other/sjm_cht.htm.
[342] Mowatt-Larssen, Rolf. "Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality?" Manuscript, Harvard Kennedy School, 2010. http://belfercenter.ksg.harvard.edu/publication/19852/al_qaeda_weapons_of_mass_destruction_threat.html.
[343] Forest, James, and Sammy Salama. Jihadist Tactics and Targeting. Jihadists and Weapons of Mass Destruction. Edited by Gary Ackerman and Jeremy Tamsett. Boc: CRC Press, 2009.

21st Century Propaganda

Beyond technical manuals, traditional media outlets and new media venues were key to al-Qaeda's efforts to propagate the religious justification for the killing of noncombatants by unorthodox methods. As Professor Gabriel Weimann explains, in 1998, less than half of the groups designated as Foreign Terrorist Organizations (FTOs) had a website; but, by the close of 1999 almost every single group had its own website.[344] [345]

On February 23, 1998, bin Laden issued his famous *fatwa* against the United States, implicitly implying an Islamic duty to deploy WMD.[346] "The ruling to kill the American and their allies – civilians and military – is an individual duty for every Muslim who can do it in any country in which it is possible to do."[347] In 1999 he proclaimed, "Acquiring weapons for the defense of Muslims is a religious duty."[348] Bin Laden's radical statements were rapidly transmitted across the Internet, and also disseminated through wire service reports and by major news outlets. His propaganda was not limited to the written word; in every year after 9/11 until his death at the hands of U.S. Navy SEALs in May 2011, bin Laden released online videos

[344] Weimann, Gabriel. Terror on the Internet: The New Arena, the New Challenges (Washington, D.C.: U.S. Institute of Peace, 2006), p. 15

[345] Hoffman, Bruce. RAND, "Congressional Testimony: The Use of the Internet by Islamic Extremists." Last modified May 2006. Accessed June 17, 2013. http://www.rand.org/content/dam/rand/pubs/testimonies/2006/RAND_CT262-1.pdf.

[346] Mowatt-Larssen, Rolf. "Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality?" Manuscript. Harvard Kennedy School, 2010. http://belfercenter.ksg.harvard.edu/publication/19852/al_qaeda_weapons_of_mass_destruction_threat.html.

[347] PBS, "Al Qaeda's Second Fatwa." Last modified February 23, 1998. Accessed June 22, 2013. http://www.pbs.org/newshour/updates/military/jan-june98/fatwa_1998.html.

[348] Mowatt-Larssen, Rolf. "Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality?" Manuscript. Harvard Kennedy School, 2010. http://belfercenter.ksg.harvard.edu/publication/19852/al_qaeda_weapons_of_mass_destruction_threat.html.

via the websites managed by al-Qaeda's media arm and to the Arabic news channel Al-Jazeera.

Al-Qaeda also employed authoritative religious surrogates to disseminate propaganda. In May 2003, extremist Saudi cleric Nasir al-Fahd wrote a 26-page *fatwa* entitled "A Treatise on the Legal Status of Using Weapons of Mass Destruction Against Infidels", which was endorsed by another extreme cleric Ali al-Khudair, a leading religious promoter of al-Qaeda.[349] Al-Fahd's *fatwa* blessed the use of WMD against infidels like Americans, but also argued the killing of fellow Muslims was permitted when one was called to Jihad. [350] [351] Nasir al-Fahd would later recant his statements in a video after his arrest by the Saudi Arabian security services. [352] Ali al-Khudair was also arrested in the same crackdown; Saudi authorities alleged al-Khudair advocated violence in his sermons and on the Internet. He too renounced violence, and the Saudi government claimed neither cleric was coerced.[353]

After 9/11, the United States' intense manhunt for al-Qaeda leadership fractured the group and forced it to rely on local network leaders to operationalize plots. As the pressure against these high value targets increased throughout the 2000s, al-Qaeda became even more dependent on surrogates and affiliate enterprises via new media platforms to spread violent messages in the hopes of

[349] PBS, "Al Qaeda's Second Fatwa." Last modified February 23, 1998. Accessed June 22, 2013. http://www.pbs.org/newshour/updates/military/jan-june98/fatwa_1998.html.
[350] Ibid.
[351] Forest, James, and Sammy Salama. Jihadist Tactics and Targeting. Jihadists and Weapons of Mass Destruction. Edited by Gary Ackerman and Jeremy Tamsett. Boc: CRC Press, 2009.
[352] Mowatt-Larssen, Rolf. "Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality?" Manuscript. Harvard Kennedy School, 2010. http://belfercenter.ksg.harvard.edu/publication/19852/al_qaeda_weapons_of_mass_destruction_threat.html.
[353] Hamdan, Amal. "Saudi cleric renounces violence." November 19, 2003. http://www.aljazeera.com/archive/2003/11/200841015258577735.html (accessed July 5, 2013).

inciting homegrown terrorists into action. In 2010, al-Qaeda in the Arabian Peninsula (AQAP), a regional franchise of al-Qaeda, released a web-accessed, English language magazine, *Inspire*. Since the original publication, in at least two of the online *Inspire* editions, the magazine's authors have called for would-be jihadists "with microbiology and chemistry degrees to develop biological or chemical toxins such as botulism, ricin, or cyanide," reflecting al-Qaeda's continued interest in pursuing a CBRN attack[354]

After the death of al-Qaeda in the Arabian Peninsula (AQAP) leader Anwar al-Awlaki by United States forces in September 2011, *Inspire* edition VIII featured an article from the deceased al-Awlaki, in which he posthumously cited six Islamic scholars to argue that the killing of civilians by chemical and biological weapons is permissible in Islam: "The use of poisons or chemical and biological weapons against population centers is allowed and is strongly recommended due to its great effect on the enemy."[355] Neither edition appears to give instructions for making CBRN devices, but they offer an urgent call to arms and proclaim the onus is on Muslim American to attack the United States. Of note, it is alleged that the 2013 Boston Marathon bombers used an *Inspire* recipe for pressure cooker bombs to build the devices they detonated in the marathon terrorist attack. The article, which appeared in the first edition of Inspire, was entitled "How to Make a Bomb in the

[354] "FBI Second Issue of Inspire Magazine Encourages Use of WMDs." Public Intelligence (blog), January 04, 2011. http://publicintelligence.net/ules-fbi-second-issue-of-inspire-magazine-encourages-use-of-wmds/ (accessed June 29, 2013).

[355] Geller, Pam. "Al-Qaeda's "Inspire" Magazine Calls for Lone-Wolf Jihad Attacks, Permits Chemical and Biological Weapons." Atlas Shrugs (blog), May 07, 2012. http://atlasshrugs2000.typepad.com/atlas_shrugs/2012/05/al-qaedas-inspire-magazine-calls-for-lone-wolf-jihad-attacks-permits-chemical-and-biological-weapons.html (accessed June 25, 2013).

Kitchen of Your Mom."[356] Nevertheless, it is as yet unclear whether the manuals for producing far more complex CBRN weapons would allow an individual with little to no scientific background to build a device capable of a mass casualty attack.

Despite the deaths of bin Laden and al-Awlaki, the Internet has kept their extremist rhetoric alive. While still a low probability event, it is troubling that a self-radicalized "lone wolf" actor with specialized expertise, access to agents, and intent to harm could fashion a CBRN device capable of inflicting serious damage. Today, al-Qaeda and its affiliates' quest to kill Americans with both conventional and unconventional terrorist acts has not diminished, while their tactics to prosecute such attacks has evolved due to steady and severe pressure from international counterterrorism efforts. Al-Qaeda is more than ever dependent on new media for survival of the network.

Failed WMD States

Thus far, this paper posited that there is no evident correlation between rising Internet users and CBRN attempted acquisition or usage; a rejection of the notional theory that diffusion of knowledge would equate to more incidents. The debate over whether or not new media is empowering terrorist groups to achieve their WMD ambitions could soon be moot. In Syria, the world is witnessing the failure of a state with the region's most expansive CW program; and nuclear-armed Pakistan appears to be trending towards greater instability, and also remains a proliferation threat.

[356] Lake, Eli. "Al Qaeda's Recipe for Pressure-Cooker Bombs." April 16, 2013. http://www.thedailybeast.com/articles/2013/04/16/al-qaeda-s-recipe-for-pressure-cooker-bombs.html (accessed June 11, 2013).

Writing in 2009, James Forest and Sammy Salama contended, "…one should not discount the possibility that in the future jihadi operatives will acquire access to CBRN agents or even ready-made weapons if favorable political circumstances arise that facilitate such transfers or theft."[357] The religious justification for WMD use propagated via the Internet could mean that CBRN terrorism among Sunni extremists has become accepted normative behavior. If so, al-Qaeda and their affiliates in Syria or Pakistan would not likely hesitate to use such a device if procured.

Syria: Al-Qaeda's Access Point for CW?

According to the British International Institute for Strategic Studies (IISS), "Syria has the largest CW arsenal in the Middle East and likely the fourth-largest in the world…it has been assessed that Syria has developed and stockpiled hundreds of tons of chemical weapons."[358] CBRN terrorism experts like Professor Charles Blair assess that "Syria may also possess an offensive biological weapons capability."[359] In addition to the precarious situation of the Assad regime using chemical weapons against civilians, there is the compounding possibility that the Syrian rebels could overtake the regime and some of the lethal agents in the Syrian stockpile could end up in the hands of terrorists that have infiltrated the rebel forces, including al-Qaeda affiliates.[360] If successful, terrorists could potentially have access to the lethal

---

[357] Forest, James, and Sammy Salama. Jihadist Tactics and Targeting. Jihadists and Weapons of Mass Destruction. Edited by Gary Ackerman and Jeremy Tamsett. Boc: CRC Press, 2009.
[358] *IISS* (blog), http://www.iiss.org/publications/strategic-comments/past-issues/volume-19-2013/april/syria-crisis-highlights-importance-of-chemical-weapons-convention/ (accessed April 01, 2013).
[359] Blair, Charles. "Fearful of a nuclear Iran? The real WMD nightmare is Syria." Bulletin of the Atomic Scientists (blog), March 01, 2012. http://thebulletin.org/fearful-nuclear-iran-real-wmd-nightmare-syria (accessed April 22, 2013).
[360] Ibid.

amounts of nerve agents including sarin and VX, as well as mustard gas, a blistering agent.[361]

The Syrian civil war is not only an internal issue; regional players such as majority Sunni states like Turkey, Jordan, and Saudi Arabia have sided with the rebels, while predominately Shi'a states like Iran and Iraq are in line with the Assad regime.[362] Aram Nerguizian from the Washington think tank the Center for Strategic and International Studies explains the looming regional crisis: "What gets lost in all the talk of Syria…is that it's located at the very epicenter of inter-Arab and Arab-Israeli politics."[363] The problem with the Sunni states' support to the rebels is that they are far less judicious with which actors receive weapons. Saudi Arabia and Qatar have sent lethal aid shipments to Jabhat al-Nusra, a Salafist group that has pledged allegiance to al-Qaeda, making it the most well armed opposition group active in Syria.[364] [365] Other regional actors with a history of supporting radical Islamic actors have enabled the extremist factions in the opposition to militarily dominate secular fighters.

---

[361] Ibid.

[362] "Syria's Crisis and the Global Response." *Council on Foreign Relations* (blog), http://www.cfr.org/syria/syrias-crisis-global-response/p28402 (accessed March 21, 2013).

[363] Kitfield, James. "The Global Dangers of Syria's Looming Civil War." *The Atlantic*, February 13, 2013. http://www.theatlantic.com/international/archive/2012/02/the-global-dangers-of-syrias-looming-civil-war/252988/ (accessed April 16, 2013).

[364] "Syrian rebel group al-Nusra Front pledges allegiance to al-Qaida." http://www.dw.de/syrian-rebel-group-al-nusra-front-pledges-allegiance-to-al-qaeda/a-16733331 (accessed March 06, 2013).

[365] Kagan, Kimberly. Institute for the Study of War, "The Smart and Right Thing in Syria." Accessed April 17, 2013. http://www.understandingwar.org/otherwork/smart-and-right-thing-syria.

Pakistan: Ticking (Nuclear) Time Bomb

Pakistan is the primary source of the nuclear terrorism threat as it hosts al-Qaeda's senior leadership, al-Qaeda sympathizers with nuclear expertise.[366] Pakistan's nuclear weapons that are not always handled with high security methods: according to both Pakistani and American sources, the Pakistan military chooses to regularly move mated nuclear weapons in modestly defended vehicles on congested public roads between multiple nuclear facilities to "keep American and Indian intelligence agencies guessing about their locations."[367] Given the presence of al-Qaeda in Pakistan, their historical nuclear weapons acquisition attempts,[368] and a history of penetrating the Pakistani security services,[369] [370] this vulnerability raises the risk level that al-Qaeda or one its alliance partners could steal a nuclear weapons, despite the difficulties associated with executing such an operation.

Pakistan and Afghanistan were key for al-Qaeda when they actively sought the capabilities to produce an improvised nuclear device. Prior to the 9/11 attacks on New York and Washington, al-Qaeda and Afghan Taliban officials met with two former Pakistani nuclear scientists in a unified effort to procure nuclear weapons.[371]

---

[366] Blair, Charles P. "Jihadists and Nuclear Weapons," in Gary Ackerman and Jeremy Tamsett, eds., Jihadists and Weapons of Mass Destruction: A Growing Threat (New York).
York: Taylor and Francis, 2009), pp. 193-238.
[367] Goldberg, Jeffrey and Ambinder, Marc. "The Ally from Hell." *The Atlantic*. 28 October, 2011. http://www.theatlantic.com/magazine/archive/2011/12/the-ally-from-hell/308730/
[368] Matthew Bunn, Yuri Morozov, et al. The U.S.-Russia Joint Threat Assessment on Nuclear Terrorism. (Working paper. Joint publication of the Belfer Center for Science and International Affairs (Harvard Kennedy School) and the Institute for U.S. and Canadian Studies (Russian Academy of Sciences), May 2011).
[369] Ewing, Philip. Report: al-Qaida infiltrated Pakistani navy." *DOD Buzz*. 31 May 2011. http://www.dodbuzz.com/2011/05/31/report-al-qaeda-infiltrated-pakistani-navy/
[370] Reuters. "Factbox: Assassination Attempts Against Pakistan's Musharraf." 6 July 2007. http://www.reuters.com/article/2007/07/06/us-pakistan-musharraf-factbox-idUSL0649978720070706.
[371] Blair, Charles P. "Jihadists and Nuclear Weapons," in Gary Ackerman and Jeremy Tamsett, eds., Jihadists and Weapons of Mass Destruction: A Growing Threat (New York).

In a U.S.-Russian joint threat assessment on nuclear terrorism, experts explained al-Qaeda's motives and historical actions:

> "Al-Qaeda has sought nuclear weapons for almost two decades. The group has repeatedly attempted to purchase stolen nuclear material or nuclear weapons, and has repeatedly attempted to recruit nuclear expertise. Al - Qaeda reportedly conducted tests of conventional explosives for its nuclear program in the desert in Afghanistan. The group's nuclear ambitions continued after its dispersal following the fall of the Taliban regime in Afghanistan. Recent writings from top al-Qaida leadership are focused on justifying the mass slaughter of civilians, including the use of weapons of mass destruction, and are in all likelihood intended to provide a formal religious justification for nuclear use." [372]

In considering how a VNSA would create an improvised nuclear device, Matthew Bunn and Anthony Wier explain that "it is worth noting that the chemistry involved in converting opium poppies to heroin…is probably roughly as complex as the chemistry required to separate uranium from research reactor fuel.[373] Of course, bin Laden's former Afghan hosts, the Taliban, are deeply intertwined in the illicit narcotics cultivation and trade in Afghanistan and are well-versed in opium conversion process.[374]

Conclusion

CBRN terrorism is often thought of as a post-modern, post-9/11 challenge, but in reality these security concerns are more than 60 years old. In 1946, theoretical physicists and Manhattan Project member J. Robert Oppenheimer, also

---

[372] Bunn, Matthew, Yuri Morozov, et al. The U.S.-Russia Joint Threat Assessment on Nuclear Terrorism. (Working paper. Joint publication of the Belfer Center for Science and International Affairs (Harvard Kennedy School) and the Institute for U.S. and Canadian Studies (Russian Academy of Sciences), May 2011).

[373] Bunn, Matthew, and Anthony Wier. 2006. Terrorist nuclear weapon construction: How difficult? Annals of the American Academy of Political & Social Science 607 (09/01): 133.

[374] Felbab-Brown, Vanda. Brookings Institute, "U.S. Counternarcotics Strategy in Afghanistan." Last modified October 21, 2009. Accessed April 17, 2013. http://www.brookings.edu/research/testimony/2009/10/21-counternarcotics-felbabbrown.

known as the father of the atom bomb, was reportedly distressed over a scenario where a few men could smuggle a nuclear weapon into New York City and detonate it without warning.[375] With other modern security matters in mind, this chapter tested whether ICT's diffusion of CBRN information had increased the probability that VNSAs would acquire and deploy a WMD device.

The empirical research confirms there is no evident correlation between rising Internet usage and CBRN attempted acquisition or deployment, a rejection of the original theory. This most likely indicates that availability of ICT is a secondary factor in determining the likelihood of VNSAs successfully executing CBRN attacks; the variables of primary importance include a permissive operating environment, freedom of movement, and direct access to skilled technicians. In this chapter, theory and probability were confronted by reality in that a terrorist group's increased access to knowledge on the Internet did not enable it to overcome the extent challenges of acquisition and deployment.

Retrospectively, the United States government's efforts to curb acts of conventional terrorism have also curbed CBRN terrorism to a degree that far outweighs any information advantage provided by VNSA access to information through ICT. However, the survival of al-Qaeda and its ideology in the face of tremendous expenditures of military, political, and economic power by the United States and its allies is a testament to the utility of ICT as a propaganda tool. Thus, insofar as those groups maintain their objective to use CBRN against civilians, ICT functions by enabling terrorists to maintain the threat of CBRN use.

---

[375] Vegar, Jose. 1998. Terrorism's new breed. Bulletin of the Atomic Scientists 54 (2) (03/01): 50.

Furthermore, the al-Qaeda case study revealed it remains plausible that ICT could enable one or more VNSAs to radicalize individuals who have already received the special training to develop or deploy CBRN, much like the Pakistani nuclear scientists in the late 1990s. Al-Qaeda's religious justification for WMD use propagated in Internet videos and in Web-based magazines may mean that CBRN terrorism among Sunni extremists is accepted as justifiable. If this is the case, VNSAs will require a nexus between their successful radicalization of skilled individuals, along with a failed state that has stockpiles of such weapons; as discussed, state collapses in Syria or Pakistan offer plausible scenarios where this nexus exists. While the findings in this chapter reinforce the hypothesis that this is a very low probability event and the data does not show an increase in such attempts, policy makers and security practitioners must be vigilant against jihadi sympathizers working in advanced sciences who could self-radicalize and use their access to conduct lone-wolf style attacks.

FINAL REMARKS

It is quite remarkable how ICT has transformed commerce, global communications, and societal interactions so dramatically in only twenty years since the modern Internet became widely accessible to individuals. As a result, all states are presented with unprecedented security vulnerabilities, and their response to shifting power differentials is paramount. This has led many analysts to proclaim that power differentials have fundamentally changed and that cyberspace ultimately will render other forms of warfare irrelevant. However, the Internet has neither fundamentally altered human nature nor the desires and competitions that fuel conflict; it is transforming the *experience* of conflict, although not necessarily the *outcomes*.

This thesis has found no conclusive data to support the notion that ICT is concurrently revolutionizing interstate, intrastate or extrastate conflict to the point whereby a weaker adversary can achieve a desired political outcome through the unique use of cyberspace. If this were the case, one would expect to see VNSAs, dissident movements, and fragile states solely using the Internet to prevail against their more powerful adversaries. At present there are no such cases. To the contrary, dominant nation states (especially authoritarians) have used ICT in concert with traditional security forces to defeat those who challenge the normal order. The prediction that the fifth domain will make other forms of warfare irrelevant, or that the Internet provides a competitive advantage for dissidents and terrorists, has not yet come to fruition.

While cyberspace adds a new virtual dimension to conflict, much like airpower added a third dimension to military conflict after World War I, cyber weapons have not yet developed to the point where they can replace weaponry in the physical domains. Some experts argue that they never will. To extend the air power analogy further, aerial systems first provided unparalleled reconnaissance capabilities before evolving into their more famous roles delivering deadly payloads. Today, cyber weapons are significantly limited and cyber warfare has not proven to be an adequate substitute for an air force, let alone an occupying force. Although as technology advances, cyber weapons could transform from auxiliary to decisive in combat, much like airpower. Alternatively, cyber warfare could be relegated to a category similar to chemical warfare: it inspires serious concerns, but has not affected the global balance of power. The latter appears more likely because of the Internet's inherent limitations in affecting the physical world.

Like all research products, this thesis is open to criticism due to the rapid pace of technological change; future events could overcome the relevance of these case studies, and new data could challenge the empirical findings. In chapter one, the cyber warfare case studies represent the use of Internet weapons by an already more powerful state, which leaves open the question of whether one can use these cases to draw firm conclusions on state power differentials. However, the other available case studies lack the documentation necessary to make them worthwhile subjects, or they do not rise to the level of warfare, which was a necessary condition for proper evaluation. Future studies of cyber warfare involving smaller states

against larger ones, or states at power parity, should be judged against the Cohen model for a more comprehensive assessment.

The Iranian case study in chapter two was completed in the fall of 2010, before the Arab Spring. While this author contends that the findings in this thesis chapter on Iran are still relevant to the Arab Spring, more detailed research is necessary, specifically on countries like Egypt (with a longstanding national identity and a robust security apparatus) as well as weaker countries, like Tunisia. Also, one could argue that while the 2009 Green Movement protests did not lead to revolutionary change, the ensuing conflict between protesters and the security forces critically undermined the regime's credibility and may have paved the way for the 2013 election of a Presidential reformer, Hassan Rouhani. This could speak volumes about the Internet's efficacy as a tool for reform, vice revolution. More observation is essential since Rouhani's election is not yet distinct from the 1997 election of ineffectual Iranian reformist Mohammad Khatami.

The conclusions drawn from the empirical research in chapter three are subject to critique since the Monterey WMD database, like all other open source datasets on CBRN terrorism, is reliant on partial information reported by news organizations, academic studies, or public government reports. To that end, CBRN terrorism incidents are also statistically insignificant events when compared to the large amount of conventional terrorism incidents, thus making the data difficult to acquire and then assess. The dearth of public information also limits case studies available for examination, but the post-9/11 media attention on al-Qaeda's WMD ambitions proved especially useful for augmenting the literature in chapter three.

The findings in this thesis have implications for how military strategists prepare for war, how diplomats engage and support like-minded groups, and how policymakers allocate funds for Defense and Homeland Security. Strategists should move quickly to build an international consensus around a definition of cyber war, vice cyber espionage or cybercrime, and establish clearly defined red lines for the military's use of the Internet in war. These actions will most likely increase predictability and avoid unintended military escalation.

Diplomats should understand the strengths and weaknesses of new media, and not rely on ICT as a panacea when engaging friendly foreign movements. More importantly, democratic states must actively encourage and cultivate open Internet policies in world forums, whenever possible. If ICT is a secondary factor in determining the likelihood of VNSAs successfully executing CBRN attacks, then policy makers should invest more resources in conventional post-9/11 counterterrorism measures to curb all methods of terrorism. Specifically, bioterror programs at the U.S. Department of Homeland Security with multi-billion dollar price tags should be thoroughly reconsidered. Much more work must be done to triage the most important security vulnerabilities, as opposed to those threats that the receive undo amount of popular attention.

Continued systematic evaluation of cyberspace's influence on conflict and security is needed to produce sound policies grounded in empirics rather than speculation. Nonetheless, it should not be a forgone conclusion that all nation states will dominate the fifth domain in the future. New media is a potent force, but it is also value-neutral and can be equally utilized by citizens, terrorists, and

governments. One particularly important question remains: if ICT has not yet upended the alignment of global power, is there a tipping point in which it might do so? For this author, such a tipping point is not probable as the Internet is fundamentally constrained from affecting the physical realm in the same coercive manner as other conventional instruments. That aside, ICT presents very real security threats that practitioners cannot ignore. As Cohen once theorized, the world may be on the precipice of an information-led transformation of war, but it is not yet at the point where one can declare that the revolution is upon us.

BIBLIOGRAPHY

"21st Century Statecraft." U.S. Department of State. http://www.state.gov/statecraft/index.htm (accessed November 19, 2010).

Abrahamian, Ervand. *Iran between Two Revolutions.* Princeton: Princeton University Press, 1982.

Ackerman, Gary, and Laura Snyder. 2002. Would they if they could? *Bulletin of the Atomic Scientists* 58 (3) (05/01).

Ackerman, Gary. *Introduction*. *Jihadists and Weapons of Mass Destruction*. Edited by Gary Ackerman and Jeremy Tamsett. Boca Raton, FL: CRC Press, 2009. pp. xi-xxxiii.

Ambider, Marc, and Jeffrey Goldberg. "The Ally from Hell." *The Atlantic*, December 2011. http://www.theatlantic.com/magazine/archive/2011/12/the-ally-from-hell/308730/?single_page=true

Arquilla, John, and David Ronfeldt. "Cyberwar is Coming!" *Comparative Strategy* 12, no. 2 (1993): 141-165.

Asal, Victor H., Gary A. Ackerman, and R. K. Rethemeyer. 2012. Connections can be toxic: Terrorist organizational factors and the pursuit of CBRN weapons. *Studies in Conflict & Terrorism* 35 (3) (03/01).

"Aum Shinrikyo: Insights Into How Terrorists Develops Biological and Chemical Weapons." manuscript, CNAS, 2012. http://www.cnas.org/files/documents/publications/CNAS_AumShinrikyo_SecondEdition_English.pdf.

A cyber-riot. 2007. *Economist 383* (8528) (05/12): 55.

"A Virtual Counter-Revolution," *The Economist*, September 4, 2010, 75-77.

Benkler, Yochai. *The Wealth of Networks*. New Haven: Yale University Press, 2006.

Blair, Charles. "Fearful of a nuclear Iran? The real WMD nightmare is Syria." *Bulletin of the Atomic Scientists* (blog), March 01, 2012. http://thebulletin.org/fearful-nuclear-iran-real-wmd-nightmare-syria (accessed April 22, 2013).

Blair, Charles P. "Jihadists and Nuclear Weapons," in Gary Ackerman and Jeremy Tamsett, eds., Jihadists and Weapons of Mass Destruction: A Growing Threat (New York).
York: Taylor and Francis, 2009), pp. 193-238.

Blair, Charles. "Radiological Ray Gun: More Buck Rogers Fantasy than Risk to Real People." *FAS Strategic Security Blog* (blog), June 20, 2013. http://blogs.fas.org/security/2013/06/radiological-ray-gun-more-buck-rogers-fantasy-than-risk-to-real-people/ (accessed July 3, 2013).

Bremmer, Ian. "Democracy in Cyberspace." *Foreign Affairs* 89 no. 6 (2010): 86-92.

Brown, Tina. "Death by Error." May 19, 2005. http://www.washingtonpost.com/wp-dyn/content/article/2005/05/18/AR2005051802083.html (accessed July 1, 2013).

Bumgarner, John, and Scott Borg. "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008." *US-CCU Special Report* (2009).

Bunn, Matthew, Yuri Morozov, et al. The U.S.-Russia Joint Threat Assessment on Nuclear Terrorism. (Working paper. Joint publication of the Belfer Center for Science and International Affairs (Harvard Kennedy School) and the Institute for U.S. and Canadian Studies (Russian Academy of Sciences), May 2011).

Bunn, Matthew, and Anthony Wier. 2006. Terrorist nuclear weapon construction: How difficult? *Annals of the American Academy of Political & Social Science* 607 (09/01).

Carr, Jeffrey. 2009. *The Evolving State of Cyber Warfare*. Phase 2. Project Grey Goose. http://fserror.com/pdf/GreyGoose2.pdf

Center for Nonproliferation Studies, "Chart: Al-Qa`ida's WMD Activities." Last modified May 13, 2005. Accessed June 5, 2013. http://cns.miis.edu/other/sjm_cht.htm.

Clarke, Richard A., and Robert Knake. *Cyber War: The next threat to national security and what to do about it*. HarperCollins, 2010: 12.

Clausewitz, Carl von. *On War*. Radford, VA: Wilder Publications, LLC, 2008.

Cohen, Eliot A. 1996. A revolution in warfare. Foreign Affairs 75 (03/01).

Cohn, Julie. "Terrorism Havens: Somalia." *Council on Foreign* (blog), June 20, 2010. http://www.cfr.org/somalia/terrorism-havens-somalia/p9366 (accessed July 28, 2013).

Cole, Juan. “The Greens in Iran are a Movement, not a Coup.” Informed Comment, (June 13, 2010) http://www.juancole.com/2010/06/the-greens-are-a-movement-not-a-coup.html (accessed December 17, 2010).

Currie, Kelley. “The Battle over Internet Freedom.” The Weekly Standard, (October 26, 2010) http://www.weeklystandard.com/blogs/battle-over-internet-freedom_512987.html (accessed October 31, 2010).

Daragahi, Borzou and Ramin Mostaghim, “Mousavi forms new political front,” Los Angeles Times, (August 16, 2009) http://articles.latimes.com/2009/aug/16/world/fg-iran-mousavi16 (accessed December 22, 2010).

-----“Defending a New Domain." Foreign Affairs, 1 Sept. 2010. Web. 2 Dec. 2013. http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

Deibert, Ronald and Rafal Rohozinski. “Liberation VS. Control: The Future of Cyberspace.” *Journal of Democracy* 21, (2010): 55.

-----Electromagnetic Spectrum." http://www.yorku.ca/eye/spectru.htm (accessed November 21, 2010).

Eslahchi, Morteza. “Tavaana Interview Transcript.” Tavaana, http://www.tavaana.org/nu_upload/Morteza_Eslahchi_En.pdf (accessed December 12, 2010).

Ewing, Philip. Report: al-Qaida infiltrated Pakistani navy.” *DOD Buzz*. 31 May 2011. http://www.dodbuzz.com/2011/05/31/report-al-qaeda-infiltrated-pakistani-navy/

“Facebook page of Mousavi.” http://www.facebook.com/#!/mousavi (accessed December 5, 2010).

-----"Fact Sheet." *U.S. Cyber Command* (blog), August, 2013. http://www.stratcom.mil/factsheets/Cyber_Command/ (accessed November 3, 2013).

Fairbanks, Charles H. "Georgia's Rose Revolution." *Journal of Democracy* 15, no. 2 (2004): 110-124.

Fathi, Asghar. "The Role of the Islamic Pulpit." *Journal of Communications* 29, no. 3 (Summer 1979): 102-105.

"FBI Second Issue of Inspire Magazine Encourages Use of WMDs." *Public Intelligence* (blog), January 04, 2011. http://publicintelligence.net/ules-fbi-second-issue-of-inspire-magazine-encourages-use-of-wmds/ (accessed June 29, 2013).

Federation of American Scientists, "Case Studies in Dual Use Biological Research." Accessed March 14, 2013. http://www.fas.org/biosecurity/education/dualuse/index.html.

Felbab-Brown, Vanda. Brookings Institute, "U.S. Counternarcotics Strategy in Afghanistan." Last modified October 21, 2009. Accessed April 17, 2013. http://www.brookings.edu/research/testimony/2009/10/21-counternarcotics-felbabbrown.

Forest, James J. F. 2012. Framework for analyzing the future threat of WMD terrorism. *Journal of Strategic Security* 5 (4) (11/01): 51.

Forest, James, and Sammy Salama. *Jihadist Tactics and Targeting*. *Jihadists and Weapons of Mass Destruction*. Edited by Gary Ackerman and Jeremy Tamsett. Boc: CRC Press, 2009.

Franklin, Curt. "How Routers Work." *How Stuff Works* (blog), http://computer.howstuffworks.com/router11.htm (accessed November 2, 2013).

"Freedom on the Net." *Freedom House* (2009), 70-75, http://www.freedomhouse.org/template.cfm?page=383&report=79 (accessed July 11, 2010).

"Freedom of the Press – Iran," *Freedom House* (20091-4), http://www.freedomhouse.org/template.cfm?page=274 (accessed July 11, 2010).

Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38, no. 2 (2013): 41-73.

Geller, Pam. "Al-Qaeda's "Inspire" Magazine Calls for Lone-Wolf Jihad Attacks, Permits Chemical and Biological Weapons." *Atlas Shrugs* (blog), May 07, 2012. http://atlasshrugs2000.typepad.com/atlas_shrugs/2012/05/al-qaedas-inspire-magazine-calls-for-lone-wolf-jihad-attacks-permits-chemical-and-biological-weapons.html (accessed June 25, 2013).

Giles, Keir. 2012. "Russia's Public Stance on Cyberspace Issues." *In 2012 4th International Conference on Cyber Conflict* (CYCON), 1 –13. Tallinn, Estonia: NATO CCD COE Publications.

Gladwell, Malcolm. "Small Change." *The New Yorker*, (October 4, 2010) http://www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell (accessed October 11, 2010).

Goldberg, Jeffrey and Ambinder, Marc. "The Ally from Hell." *The Atlantic*. 28 October, 2011. http://www.theatlantic.com/magazine/archive/2011/12/the-ally-from-hell/308730/ (accessed July 1, 2013).

Hamdan, Amal. "Saudi cleric renounces violence." November 19, 2003. http://www.aljazeera.com/archive/2003/11/200841015258577735.html (accessed July 5, 2013).

Hannabuss, Stuart. 2008. Terror on the internet: The new arena, the new challenges. *Journal of Political Marketing* 7 (1) (03/01): 99.

Hare, Forrest. 2007. "Five Myths of Cyberspace and Cyberpower." SIGNAL Magazine (June). http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=1333&zoneid=209 (accessed September 29, 2013).

Herrmann, Steve. "Social Media in Iran," *BBC*, June 16, 2009, Tuesday; online edition, http://www.bbc.co.uk/blogs/theeditors/2009/06/social_media_in_iran.html (accessed November 1, 2010).

Herzog, Stephen. 2011. Revisiting the Estonian Cyber Attacks: Digital threats and multinational responses. Journal of Strategic Security 4 (2) (05/01): 50.

Hessel, Andrew, Marc Goodman, and Steven Kotler. 2012. Hacking the President's DNA. *Atlantic Monthly (10727825)* 310 (4) (11/01): 82.

Hoffman, Bruce. "CBRN Terrorism Post 9/11," in Weapons of Mass Destruction and Terrorism, eds. Russell D. Howard and James Forest (New York: McGraw-Hill, 2007).

Hoffman, Bruce. RAND, "Congressional Testimony: The Use of the Internet by Islamic Extremists." Last modified May 2006. Accessed June 17, 2013. http://www.rand.org/content/dam/rand/pubs/testimonies/2006/RAND_CT262-1.pdf.

Hollis, David. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal*. http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008 (accessed October 15, 2013).

IISS (blog), http://www.iiss.org/publications/strategic-comments/past-issues/volume-19-2013/april/syria-crisis-highlights-importance-of-chemical-weapons-convention/ (accessed April 01, 2013).

International Telecommunication Union, "ICT Facts and Figures." Accessed June 14, 2013. http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf.

"Internet Basics." Florida Center for Instructional Technology. http://fcit.usf.edu/Internet/chap1/chap1.htm (accessed November 19, 2010).

Ivanova, Kate, and Todd Sandler. 2007. CBRN attack perpetrators: An empirical study. *Foreign Policy Analysis* 3 (4) (10/01): 273.

Ivanova, Kate, and Todd Sadler. "CBRN Incidents: Political Regimes, Perpetrators and Targets." *Terrorism and Political Violence*. No. 3 (2006): pp. 423-448.

Kagan, Frederick. "It's Not a Cold War." *National Review Online*, August 20, 2008. http://www.aei.org/article/foreign-and-defense-policy/regional/europe/its-not-a-cold-war/ (accessed October 15, 2013).

Kagan, Kimberly. Institute for the Study of War, "The Smart and Right Thing in Syria." Accessed April 17, 2013. http://www.understandingwar.org/otherwork/smart-and-right-thing-syria.

Kazi, Reshmi. 2011. The correlation between non-state actors and weapons of mass destruction. *Connections (18121098)* 10 (4) (09/01).

Keddie, Nikki R. *Modern Iran: Roots and Results of Revolution.* 2 ed. New Haven: Yale University Press, 2006.

Kelly, Henry, and Michael Levi. Federation of American Scientists, "Weapons of Mass Disruption." Last modified November 2002. Accessed August 5, 2013. http://www.fas.org/ssp/docs/021000-sciam.pdf.

Kelly, John and Bruce Etling. "Mapping Iran's Online Public." *Berkman Center Research Publication* no. 2008-01 (2008): 1-35.

Kitfield, James. "The Global Dangers of Syria's Looming Civil War." *The Atlantic*, February 13, 2013. http://www.theatlantic.com/international/archive/2012/02/the-global-dangers-of-syrias-looming-civil-war/252988/ (accessed April 16, 2013).

Krebs, Brian. "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks." *The Washington Post* 16 (2008).

Krepinevich, Andrew F. *Cavalry to Computer: The Pattern of Military Revolutions*. National Affairs, 1994.

Kristof, Nicholas. "Tear Down This Cyberwall!" *New York Times*, (June 17, 2009) http://www.nytimes.com/2009/06/18/opinion/18kristof.html (accessed October 13, 2010).

Kuehl, Daniel "The Information Revolution and the Transformation of Warfare," in Karl de Leeuw & Jan Bergstra editors, *The History of Information Security* (Amsterdam, Netherlands: Elsevier, 2007).

Lake, Eli. "Al Qaeda's Recipe for Pressure-Cooker Bombs." April 16, 2013. http://www.thedailybeast.com/articles/2013/04/16/al-qaeda-s-recipe-for-pressure-cooker-bombs.html (accessed June 11, 2013).

Landler, Mark, and John Markoff. "Digital Fears Emerge After Data Siege in Estonia." New York Times, May 29, 2007. http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0 (accessed September 26, 2013).

Langø, Hans-Inge. *Slaying Cyber Dragons: Competing Approaches to Cyber Security*. Working paper, Norwegian Institute of International Affairs, 2013.

Lawson, Sean. "Beyond cyber-doom: Cyberattack Scenarios and the Evidence of History." *Mercatus Center George Mason University Working Paper* 11-01 (2011).

Leitenberg, Milton. 2009. The threat of bioterrorism, real and imagined. *World Politics Review (19446284)* (10/27).

Levi, Michael A., and Henry C. Kelly. 2002. Weapons of mass disruption. *Scientific American* 287 (5) (11/01): 76.

Macfarlane, Allison. "All Weapons of Mass Destruction Are Not Equal," Audit of the Conventional Wisdom Series, Center for International Studies, MIT, July 2005.

Mahnken, Thomas. *Cyberwar and Cyber Warfare*. *America's Cyber Future, Volume II*. CNAS, 2011. https://www.cnas.org/files/documents/publications/CNAS_Cyber_VolumeII_2.pdf (accessed September 30, 2013).

Majd, Hooman. "Think Again: Iran's Green Movement." *Foreign Policy*, (January 6, 2010) http://www.foreignpolicy.com/articles/2010/01/06/think_again_irans_green_movement (accessed January 6, 2010).

McComb, Jonathan M. 2013. Closing Pandora's Box: The threat of terrorist use of weapons of mass destruction. *Global Security Studies* 4 (1) (02/01): 71.

McConnell, Mike. Cyber Insecurities: The 21st Century Threatscape. *America's Cyber Future*, Volume II. CNAS, 2011. https://www.cnas.org/files/documents/publications/CNAS_Cyber_VolumeII_2.pdf (accessed September 30, 2013).

McGraw, Gary, and Nathaniel Fick. *Separating Threat from the Hype: What Washington Needs to Know about Cyber Security*. *America's Cyber Future, Volume II*. CNAS, 2011.

https://www.cnas.org/files/documents/publications/CNAS_Cyber_VolumeII_2.pdf (accessed September 30, 2013).

McNaugher, Thomas L. 2007. The real meaning of military transformation: Rethinking the revolution: Review essay. Foreign Affairs 86 (1) (01/01): 140.

Memarsadeghi, Mariam. "Technology Fund: Investing in the Green Movement for Democracy." *International Perspectives on the Middle East* (2010).

Milani, Abbas. "The Green Movement." United States Institute of Peace, http://iranprimer.usip.org/resource/green-movement (accessed December 5, 2010).

Militant Islamic Political Activism on the Worldwide Web, Foreign Broadcast Information Service, "RAND." Last modified December 19, 2000. Accessed August 5, 2013. http://130.203.133.150/showciting;jsessionid=1F0207FB4B21FF92EEE26C53ADD49CC7?cid=13454017.

Miller, Robert A., and Daniel T. Kuehl. *Cyberspace and the 'First Battle' in 21st-century War*. Center for Technology and National Security Policy, National Defense University, 2009.

Monterey WMD Terrorism Database. http://wmddb.miis.edu/ (accessed July 2, 2013).

Mooney, Alexander. "CNN Politics." *Obama promotes foreign policy cred in new ad* (blog), July 15, 2008. http://politicalticker.blogs.cnn.com/2008/07/15/obama-promotes-foreign-policy-cred-in-new-ad/ (accessed March 5, 2013).

Morozov, Evgeny. "How dictators watch us on the web." *Prospect*, (November 18, 2009) http://www.prospectmagazine.co.uk/2009/11/how-dictators-watch-us-on-the-web/ (accessed September 18, 2010).

Mousavi, Mir Hossein. Campaign Website. http://www.mir-hosseinmousavi.com/policies.html (accessed December 1, 2010).

Mowatt-Larssen, Rolf. "Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality?" manuscript, Harvard Kennedy School, 2010. http://belfercenter.ksg.harvard.edu/publication/19852/al_qaeda_weapons_of_mass_destruction_threat.html.

-----*NATO Cooperative Cyber Defense Centre of Excellence*, https://www.ccdcoe.org/ (accessed November 6, 2013).

Nye, Jr., Joseph. *Cyber Power*. Manuscript, Harvard Kennedy School, 2010. http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

Nye, Jr., Joseph. Harvard Belfer Center, "Cyber War and Peace." Last modified April 10, 2012. Accessed October 6, 2013. http://belfercenter.ksg.harvard.edu/publication/21937/cyber_war_and_peace.html?breadcrumb=/project/67/explorations_in_cyber_international_relations.

Nye, Jr., Joseph. *The Future of Power*. New York City: Public Affairs, 2011.

PBS, "Al Qaeda's Second Fatwa." Last modified February 23, 1998. Accessed June 22, 2013. http://www.pbs.org/newshour/updates/military/jan-june98/fatwa_1998.html.

Peterson, Britt. "A Forgotten Civil Society." *Foreign Policy* (June 7, 2010) http://www.foreignpolicy.com/articles/2010/06/07/a_forgotten_civil_society (accessed June 25, 2010).

Pitcairn, Daniel. "A Missed Chance for NATO's Cybersecurity Future." *Defense One*, October 23, 2013. http://www.defenseone.com/ideas/2013/10/missed-chance-natos-cybersecurity-future/72542/?oref=d-interstitial-continue (accessed October 30, 2013).

Reuters. "Factbox: Assassination Attempts Against Pakistan's Musharraf." 6 July 2007. http://www.reuters.com/article/2007/07/06/us-pakistan-musharraf-factbox-idUSL0649978720070706

Rid, Thomas. 2013. Cyberwar and Peace. *Foreign Affairs* 92 (6) (11/01): 77.

Sadjadpour, Karim. "Off the Political Radar," *Qantara*, (2010) http://en.qantara.de/webcom/show_article.php/_c-476/_nr-1343/i.html (accessed December 12, 2010).

Schmitt, Gary. "The Forgotten War." *AEI Ideas* (blog), August 07, 2013. http://www.aei-ideas.org/2013/08/the-forgotten-war/ (accessed November 7, 2013).

Segal, Adam. "What to Read on Cybersecurity." *Foreign Affairs* (blog), November 12, 2012. http://www.foreignaffairs.com/features/readinglists/what-to-read-on-cybersecurity (accessed October 6, 2013).

Shachtman, Noah. "http://www.wired.com/dangerroom/2009/03/georgia-blames/" *WIRED*, March 11, 2009. http://www.wired.com/dangerroom/2009/03/georgia-blames/ (accessed October 15, 2013).

Shakarian, Paulo. "The 2008 Russian Cyber Campaign against Georgia." *Military Review-English Edition* 91, no. 6 (2011).

Shirky, Clay. "The Net Advantage." *Prospect*, December 11, 2009, http://www.prospectmagazine.co.uk/2009/12/the-net-advantage/ (accessed September 12, 2010).

Silverman, Jacob. "Could hackers devastate the U.S. economy?" *How Stuff Works* (blog), http://computer.howstuffworks.com/die-hard-hacker1.htm (accessed November 2, 2013).

Skocpol, Theda. "Rentier State and Shi'a Islam in the Iranian Revolution." *JSTOR*: 265-267, http://www.strongwindpress.com/pdfs/TuiJian/SkocpolRentierStateIran.pdf (accessed July 14, 2010).

Slaughter, Anne-Marie. "America's Edge." *Foreign Affairs*, (January/February 2009), http://www.foreignaffairs.com/articles/63722/anne-marie-slaughter/americas-edge (accessed December 8, 2010).

Sreberny-Mohammadi, Annabelle and Ali Mohammadi. *Small Media, Big Revolution.* Minneapolis: University of Minnesota Press, 1994.

Sublette, Carey. "Section 5.0 Effects of Nuclear Explosions." *Nuclear Weapons Archive* (blog), May 15, 1997. http://nuclearweaponarchive.org/Nwfaq/Nfaq5.html (accessed June 5, 2013).

Sullivan, Andrew. "The Revolution Will Be Twittered." *The Atlantic*, (June 13, 2009) http://andrewsullivan.theatlantic.com/the_daily_dish/2009/06/the-revolution-will-be-twittered-1.html (accessed December 30, 2010).

"Syrian rebel group al-Nusra Front pledges allegiance to al-Qaida." http://www.dw.de/syrian-rebel-group-al-nusra-front-pledges-allegiance-to-al-qaeda/a-16733331 (accessed March 06, 2013).

"Syria's Crisis and the Global Response." *Council on Foreign Relations* (blog), http://www.cfr.org/syria/syrias-crisis-global-response/p28402 (accessed March 21, 2013).

Szrom, Charlie. "Iran Tracker." American Enterprise Institute, (May 13, 2009) http://www.irantracker.org/tehran/mir-hossein-mousavi-biography-and-campaign-news (accessed December 5, 2010).

Tehranian, Majid. *International Journal of Middle East Studies* (1995), http://www.jstor.org/pss/176378 (accessed July 17, 2010).

Terrorism and weapons of mass destruction. 2007. *Homeland Defense Journal* 5 (4) (04/01): 16.

----- The American Enterprise Institute, "The War in the Caucasus: An Initial Assessment." Last modified August 13, 2008. Accessed November 7, 2013. http://www.aei.org/files/2008/08/13/20080813_PowerpointPresentation.pdf.

-----The Harriman Institute, "Columbia University." Accessed November 7, 2013. http://www.columbia.edu/cu/news/global/images/Post-SovietTimeline.pdf.

"The World Trade Center Bombers," in Jonathan B. Tucker, ed., Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons (Cambridge, MA: MIT Press, 2000), pp.185-206.

"Twitter page of Mousavi." http://twitter.com/MirTweets (accessed December 5, 2010).

U.S. Department of Commerce, "American Fact Finder: Census Data." Accessed August 5, 2013. http://factfinder2.census.gov/faces/nav/jsf/pages/index.xhtml.

Vegar, Jose. 1998. Terrorism's new breed. *Bulletin of the Atomic Scientists* 54 (2) (03/01): 50.

Weimann, Gabriel. Terror on the Internet: The New Arena, the New Challenges (Washington, D.C.: U.S. Institute of Peace, 2006), p. 15

Weinberger, David. "Gladwell discovers it takes more than 140 characters to overturn a government." Available from http://www.hyperorg.com/blogger/2010/10/02/gladwell-discovers-it-takes-more-than-140-characters-to-overturn-a-government/. Internet; accessed 16 October 2010.

Wellerstein, Alex. *Nukemap* (blog), http://nuclearsecrecy.com/nukemap/ (accessed June 3, 2013).

AUTHOR'S BIOGRAPHY

Megan Leann Ortagus is a Master of Arts candidate in Global Security Studies at the Johns Hopkins University. She graduated with a Bachelor's Degree in Music from Southeastern University in 2005. Ms. Ortagus was born in Florida in 1982. She is married to Farook Ahmed; they presently reside in Arlington, Virginia.